CampusQuest: Motivating Computer Science Students for Cybersecurity from Day One

Luca Pöhler[a], Marko Schuba[b], Tim Höner[c], Sacha Hack[d] and Georg Neugebauer[e]
Department of Electrical Engineering and Computer Science, FH Aachen University of Applied Sciences,
Eupener Str. 70, 52066 Aachen, Germany

Keywords: Gamification, Challenges, CTF, IT Security, Cybersecurity, Cybersecurity Games, CTFd.

Abstract: The increasing significance of information technology (IT) security in modern life and the rising number of cybersecurity regulations and legislation are creating a high demand for IT security experts, which is currently unmet, resulting in numerous vacancies. To address this shortage of skilled professionals, it is crucial to cultivate early interest among students. In the present study, the game-based system CampusQuest is introduced as a tool to engage students in cybersecurity from the outset and to stimulate their ambition in this field. The system is based on the concept of solving challenges, similar to the format of so-called Capture the Flag competitions. However, the challenges have been adapted to align with the specific context of a university campus, combining various additional elements. CampusQuest incorporates physical elements into the challenges, which are distributed permanently across the campus and motivate individuals to participate. Additionally, the system has been enhanced with a mechanism to prevent the dissemination of solutions. The system has been implemented in a prototype form and currently comprises eleven challenges of varying degrees of difficulty, which is designed to facilitate the introduction of the subject to first-year students.

1 INTRODUCTION

The demand for cybersecurity expertise and workforce continues to grow. A study of ISC2 states that roughly four million additional cybersecurity professionals are needed worldwide (ICS2, 2023). The profession needs to almost double to be at full capacity. Looking at the German workforce market, for example, the number of open positions for IT professionals has reached 150,000 in 2023 (Statista Research Department, 2023), of which 71% fall into the category of cybersecurity (Schindler, 2023). With recent national and international events and legislation, the demand for IT security professionals is set to increase in the coming years. For example, the NIS2 Directive will present additional cybersecurity challenges for EU companies in the coming years, leading to additional efforts and workforce (European Parliament, 2023).

Notwithstanding the acknowledged shortage of experts in this field, many computer science students at the outset of their studies remain uncertain about their future areas of interest. Aachen University of Applied Sciences currently offers a selection of 33 elective modules as part of its Bachelor in Computer Science degree program. These modules can be elected by students in their fourth or fifth semester of studies. A significant proportion of first and second-year students are yet to determine which of the available modules they will select. Also, higher education offerings based on gamification are proving highly popular. In the domain of IT security, for instance, Capture the Flag (CTF) projects are provided with the objective of stimulating and deepening students' interest in the subject matter and supporting their decision-making process regarding cybersecurity modules. Such offers are, however,

[a] https://orcid.org/0009-0007-5648-0559
[b] https://orcid.org/0000-0002-3302-3060
[c] https://orcid.org/0009-0006-0224-6292
[d] https://orcid.org/0000-0001-6624-0486
[e] https://orcid.org/0009-0008-0927-2324

Pöhler, L., Schuba, M., Höner, T., Hack, S. and Neugebauer, G.
CampusQuest: Motivating Computer Science Students for Cybersecurity from Day One.
DOI: 10.5220/0013164800003899
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 254-262
ISBN: 978-989-758-735-1; ISSN: 2184-4356

time-limited and frequently only made known to students in higher semesters.

To foster early engagement with cybersecurity among computer science students and provide flexibility beyond the confines of pre-established CTF events, an innovative CampusQuest platform has been developed to facilitate the creation and dissemination of CTF-inspired challenges. The challenges are intended to be made physically available on the campus in perpetuity and in a variety of locations, and they are designed to serve as a kind of treasure hunt, capturing the interest of students in IT security from the earliest days of their studies. Thematic content of the challenges includes cryptographic puzzles, penetration testing tasks, or investigations related to digital forensics. The challenges are designed to encompass varying degrees of difficulty, facilitating a gradual introduction to the subject matter for beginners without prior knowledge.

The remainder of the paper is organized as follows. Section 2 provides an overview of the fundamentals of CTFs and gamification. The current state of the art in gamification within the cybersecurity domain is described in section 3. Section 4 introduces the developed CampusQuest platform. Chapter 5 outlines the challenges that have been designed so far, with two selected for more detailed analysis. Chapter 6 summarizes the findings and offers a prospective view of the project's future.

2 BACKGROUND

2.1 Gamification

Gamification can be defined as the utilization of design elements that are characteristic of games in contexts that are not inherently related to gaming (Deterding et al., 2011). Gamification involves packaging non-game learning content in a way that makes it more engaging and accessible. This allows games, which are typically designed to satisfy hedonistic entertainment or pastime motives, to be utilized for the purpose of achieving something else, in this case, the success of the learning process (Diercks and Kupka, 2013). This exploits the human propensity for play to focus attention and commitment on a specific task or learning objective. This can lead to enhanced learning outcomes, increased motivation, greater autonomy, and more sustainable learning results (Jacob and Teuteberg, 2017; Kim et al, 2018).

Motivation represents the most crucial factor influencing the success of gamification. The most significant motivational factors that contribute to success are self-determination and autonomy, perfectionism and goal orientation, as well as social reference and significance. Additionally, the concept of flow, as postulated by Mihaly Csikszentmihalyi (Csikszentmihalyi, 2019), is frequently invoked. The concept of flow, or flow channel, describes a state of complete immersion in an activity. This state of equilibrium is achieved when the fear of being overwhelmed and the boredom resulting from being under-stimulated are balanced, and the individual feels content. In this state, learning outcomes are enhanced, and motivation and engagement are greater. Therefore, it is important that games have difficulty levels that are adapted to the abilities of the participants. This can be done in gamification in a more individualized manner than in traditional frontal teaching (Gonzales-Scheller, 2013).

The CampusQuest platform is designed to motivate students with varying backgrounds and abilities in IT security to achieve initial learning outcomes. It is structured similarly to a CTF to facilitate this.

2.2 Capture the Flag

The concept of CTFs has been in existence for a considerable length of time. Its applications are manifold and diverse. The fundamental principle remains constant, however, and is based on the competition between at least two teams, each attempting to steal the flag of the opposing team. The principle has its roots in ancient military tactics, as evidenced by the necessity for the Roman Legions to defend their standards from enemy forces. Contemporary applications include military exercises, video games, and paintball competitions (Hacking Academy, 2024).

In the context of gamification in education and training, this principle has been applied to cybersecurity and other learning contexts. The first CTF competition was held in Texas in the 1990s at the HoHoCon. In 1996, the concept was introduced at the largest cybersecurity conference in the USA, DEFCON, where it gained worldwide recognition (CyberVista, 2020).

Since that time, cybersecurity-focused CTFs have gained increasing popularity worldwide. In Jeopardy CTFs, participants attempt to solve specific tasks, frequently searching for a flag represented by a sequence of characters. The discovery of a flag is then rewarded with points, with the number of points awarded varying depending on the task's complexity. The participant or team with the highest score at the end of the competition is declared the winner. Jeopardy-CTF is the most common format of cybersecurity-focused CTFs (Chung, 2024a; Ctftime, 2024).

To provide a visual representation of the current point standings for teams or participants and to foster a sense of competition, scoreboards are utilized in CTF events, as well as in numerous other competitive settings. Typically, the scoreboard displays the current standings of the participants and a ranking of the overall leader. This is arguably the most crucial design element, preceding even the badges and point system, in determining the success of the competition (Toda et al., 2018).

3 RELATED WORK

The concept of gamification is widely used in commercial contexts across a range of industries. The most popular features of gamification are those related to fitness apps. Many providers implement primarily, as is typical of games, reward mechanisms. For example, apps such as “Nike Run Club” and “Huawei Health” allow users to earn points and medals through specific tasks or activities. Additionally, these apps employ elements from games in their design and structure (Nike, 2024; Huawei, 2024).

In the field of education, tools such as Kahoot and Mentimeter have gained significant traction, particularly in the wake of the global COVID-19 pandemic. In the preceding year alone, 24 million users engaged in Kahoot quizzes, while 163 million participated in those of Mentimeter (Kahoot, 2024; Mentimeter, 2023).

The gamification of cybersecurity has been in use for some time. The number of Capture the Flag (CTF) events is substantial, as is the number of attendees. In some cases, these events are held locally or within the organization. There are also numerous online providers of IT security CTFs and IT security laboratory environments. This section will introduce some of these providers.

3.1 HackTheBox

HackTheBox (HTB) is one of the foremost gamified platforms for professional development, certification, and talent assessment in the cybersecurity domain. In 2023, the company announced that it had reached two million users worldwide (Ophie, 2023). Currently, in addition to numerous CTF events, there are also over 1,000 so-called virtual labs available for the purpose of enhancing one's cybersecurity capabilities (HackTheBox, 2024a). Additionally, the HTB Academy offers online courses on IT security, as well as “Hacking Battlegrounds,” which are multiplayer challenges. HTB offers a basic subscription plan that is free of charge. However, to access all challenges and features, a paid subscription is required. Additionally, courses from the HTB Academy that are finished with certificates are also available for a fee (HackTheBox, 2024b).

3.2 TryHackMe

TryHackMe represents a significant competitor for HackTheBox. The two platforms offer similar services, however, TryHackMe places a greater emphasis on “learning paths,” which provide step-by-step instruction in IT security knowledge across selected categories. Naturally, the platform also offers traditional CTF challenges with competitive elements and rankings, as well as the "King of the Hill" format, in which players assume the roles of attacker or defender and compete against each other. The platform offers a “skills matrix” that indicates the user's progress in various domains and enables the confirmation of this progress through the issuance of certificates. Additionally, other gamification elements are employed, such as progress badges. Like the majority of providers in this field, TryHackMe is based on a freemium model. Registration is free, but the functionality is limited. To utilize all features, a premium subscription must be purchased, which requires a monthly payment (TryHackMe, 2024).

3.3 PentesterLab

PentesterLab is another online learning platform for IT security. The focus of the individual challenges is on the underlying vulnerabilities. With an annual subscription, users gain access to all exercises, as well as videos on the exercises and certificates confirming the completion of all tasks (PentesterLab, 2024).

3.4 CyberDefenders

In addition to numerous other providers of traditional IT security challenges on the internet, which typically focus on compromising systems, there are also websites that specialize in defending and analyzing security incidents. CyberDefenders is one such website that offers the “CyberRange” in addition to training and certification courses on the subject of blue teaming. In the domain of IT security, the term "blue team" is used to refer to the cybersecurity experts whose responsibility it is to defend the IT infrastructure against attacks (Luber and Schmitz, 2020). The “CyberRange” offers a variety of laboratories in which users can learn to analyze malware, conduct network and endpoint forensics, and other skills. A distinction is made between freely available and so-called PRO-Labs. The latter necessitate a monthly subscription (CyberDefenders, 2024). CyberDefenders incorporates elements of gamification, such as leaderboards and badges, to encourage regular participation in challenges. Additionally, users are permitted to create their own labs, which can then be solved by other members.

3.5 Portswigger Academy

Portswigger is primarily recognized for its Burp Suite program, which enables IT security professionals to assess network traffic and applications. The Portswigger WebSecurity Academy provides a platform for the acquisition of knowledge regarding IT security concepts in the context of web security. The main focus is on training the usage of the Burp Suite tool and its functions. The Portswigger Academy also incorporates elements of gamification, such as badges and a progress bar indicating the number of labs completed by the user. While the learning resources are freely available, in some cases, a Burp Suite Professional license may be required, which incurs a fee (PortSwigger, 2024).

The presented websites and challenges are already well-established and offer excellent learning opportunities for those interested in IT security. Therefore, the objective of this paper is not to improve or surpass these sites, but rather to focus on engaging students at an earlier stage of their career and motivate them to pursue independent learning, for example, by exploring the aforementioned websites, participating in challenges, or engaging with cybersecurity modules at the university.

4 CAMPUSQUEST PLATFORM

4.1 Requirements

The CampusQuest system differs from traditional CTFs in that it has a permanent and physical character. To this end, 3D-printed elements have been created that can be mounted at the university campus and serve as both entry points and data collection points for challenges. The physical visibility of the CampusQuest elements helps to attract the attention of students and arouses their curiosity.

A crucial requirement for this project was the ability to administer the challenges in a unified and structured manner and being able to put it under version control. This enables the iterative development of individual challenges and ensures the long-term sustainability of the project. Furthermore, it facilitates the creation and maintenance of challenges, thereby streamlining the process for future administrators of the CampusQuest system, making it easier for them to contribute to the project.

The fundamental structure of the CampusQuest platform at the university is comprised of a CTF server, a customized challenge management system, and a conceptual framework for utilization. Additionally, a series of illustrative challenges have been designed to demonstrate the integration of challenges into the system, the incorporation of challenges into the physical environment, and the implementation of challenges in a tangible manner. Furthermore, a prototype for a flag management system has been developed to prevent the dissemination of solutions among students.

The challenges were selected in a manner that reflects the content of potential course modules within the computer science degree program at the university, or alternatively, serves to stimulate interest in these areas. The difficulty level was deliberately set at a relatively low threshold to avoid overwhelming those with limited experience. As the initial challenges are intended to serve as a template or exemplar for a subsequent, integrated challenge series, a variety of formats were selected, drawing upon existing CTFs or based on insights gained from the computer science curriculum. To identify potential issues or areas for improvement, a small group of students was consulted during the pre-testing phase.

In order to meet the requirement of a physical starting point on campus, elements with the CampusQuest logo and a QR code were produced using a 3D printer, thus ensuring the elements had a degree of visual recognition. The linked web interface can be used to disseminate passwords, text elements, or links to data downloads. Alternatively, modular CampusQuest boxes are currently being developed that can accommodate small devices for wireless or USB interaction with students.

4.2 Technologies Employed

4.2.1 Existing Software

The presented version of CampusQuest employs a variety of freely available technologies, notably CTFd and ctfcli for server and challenge administration, Docker for server execution, Github for code management, and Python and Rust for programming. Some or these technologies will be briefly described in the following sections.

CTFd is a framework designed for the creation of CTF events with the majority of CTFd being written in Python and utilizing the Flask framework (Chung, 2024b). In the CampusQuest context the CTFd website serves as the front end for both user interaction and administrative tasks. Furthermore, it encompasses the display and monitoring of challenges and flags, as well as a scoreboard that allows participants to gauge their individual point totals. Additionally, participants can utilize their accumulated points to unlock hints for solving challenges (Chung, 2024b; Chung, 2017).

While the free version of CTFd was generally suitable for use as a CampusQuest platform, it was also evident that certain limitations existed, necessitating the implementation of extensions. Given the necessity of adding or modifying challenges on an ongoing basis, an alternative solution for the administration of challenges was required. To this end, the command-line program ctfcli, also developed by CTFd, was employed. It offers the ability to install, synchronize, and export challenges individually. Text-based challenge configuration files are utilized, facilitating straightforward creation and administration. Additionally, remote computer commands can be executed (CTFd, 2024a; CTFd, 2024b).

In order to implement the programming tasks, the decision was taken to use Python and Rust. Python is a contemporary, interpreted programming language that emphasizes object-oriented, functional, and imperative programming. Python is a popular choice among beginners and advanced programmers alike due to its readability and ease of use (Kelly, 2019). The additional use of the compiled language Rust was motivated by the superior runtime performance and the fact that Python programs are easily human-readable. This approach has the advantage that participants will find it very difficult to reverse-engineer the flag generation scripts (Müller et al., 2000).

4.2.2 Self-Developed Software

In order to facilitate the creation of personalized, or at the very least, reusable flags, a flag plugin with new flag types was developed. To this end, the software CTFd has been augmented with customized functions that facilitate the creation and verification of personalized and time-based flags. As an example, the creation of flags may include the option of adding a supplementary time stamp, which can limit the duration of use. Similarly, the username can be incorporated into the generation function, thereby ensuring that a flag can only be used by the correct user. This results in four distinct flag types, depending on whether time and/or the user are included in the generation: static flags, dynamic time-based flags, dynamic user-based flags, and dynamic time- and user-based flags.

4.3 Creation of CampusQuest Challenges

New challenges may be created and added in one of two ways: either via the user interface of the CTFd server or using ctfcli. However, the latter method is recommended, as it allows challenges to be planned and created without direct access to the CTFd server. This should facilitate the creation of challenges for a wider audience, as it removes the need for familiarity with CTFd or the ability to make corrections.

The administration of the system via ctfcli is based on configuration files that can be created and loaded into the repository using any text editor. Examples of configuration data include the name of the challenge, the name of the author, the challenge category (e.g., “digital forensics”), and a brief description. The configuration value “type” denotes the type of challenge, which may be designated as “standard” or “dynamic,” among other options. In the case of the "standard" challenge, all participants are awarded the specified number of points. In contrast, a “dynamic” challenge entails a reduction in the point value as additional participants solve the challenge. The objective is to provide a more substantial reward for the expeditious mastering of particularly difficult challenges. The “flags” parameter is capable of accepting either simple strings or dictionaries. In the event that the flag is entered as a string, a static flag will be generated. Furthermore, dynamic flags may be entered. Should one wish to provide a file, this may be done via the “files” parameter. Additionally, tags may be specified in order to provide participants with information regarding the contents of the challenges. Hints may be specified in a manner analogous to flags, and are intended to serve as guidance for participants. These may be assigned a cost in the form of points.

In order to guarantee the quality of the challenges and the seamless functionality of the CampusQuest server, a process for implementing software changes has been developed. This process concerns the addition or modification of challenges, as well as plugins and other alterations to the server. It employs the DevOps principle of feature branches. The current, tested, and functional version of the challenges is located on the main branch of Git. This is subsequently utilized by the production server to load the challenges onto the CTFd container, which is accessible to all students.

Should a supervisor or other relevant individual wish to develop and provide a new challenge, it is first uploaded to a feature or development branch in Git. Next, the challenge is transferred to a distinct testing server. This server is not accessible to all students. Subsequently, the new challenges are subjected to a preliminary examination by the set of students belonging to the IT security club at the university. This process allows for the discovery and removal of bugs or difficulties before the challenge is released to the entire student body. Once the challenges have been optimized, all members of the club are invited to evaluate them. The decision is then made as to whether the challenges will be incorporated into the operational system. If this is the case, the relevant feature branch can be merged into the main branch, and the changes can be loaded onto the operational server. Additionally, the physical element representing the challenge needs to be mounted on the campus.

5 CAMPUSQUEST CHALLENGES

In addition to the CampusQuest backend, several challenges have been implemented or adopted as part of this project. These serve as a foundation and exemplar for the subsequent implementation of additional challenges. Table 1 on the next page provides an overview of the challenges created or integrated so far.

As can be observed in the table, the flags associated with the challenges are typically static. The rationale behind this approach is to minimize the initial expenditure associated with the creation of challenges. While the generation of flags in a dynamic manner at a later stage is a viable option for many challenges, it is not a practical solution for others, such as the RDP bitmap, for which dynamic flags would require unreasonable development efforts. The suitability of this approach will be determined over time as more experience is gained.

The following subsections will provide a more detailed analysis of two of the eleven CampusQuest challenges that have already been implemented: “Puzzle Frenzy” and “Weird Knocking Noise.”

5.1 Puzzle Frenzy

The Remote Desktop Protocol (RDP) employs the use of bitmap caches with the objective of optimizing the transmission process, when transferring screen content from one computer to another. Discrete portions of the display are cached, thus obviating the necessity for repeated transmission of screen parts that are currently static (Microsoft, 2021). The default location for the RDP bitmap cache is as follows: C:\Users\<USER>\AppData\Local\Microsoft\Terminal Server Client\Cache\. The cache can be utilized by digital forensics investigators to reconstruct potential screen content of a computer. However, the files must first be processed. The open-source tool bmc-tools can be used for this purpose (Bmc-tools, 2024). It generates readable “.bmp” files from file “bcache.bmc” and the corresponding “bin” files found in the cache directory. At this point, one may attempt to manually reassemble the individual components or alternatively employ specialized software, such as the RDPCacheStitcher tool (BSI, 2024). This tool facilitates structured assembly of the components and provides immediate feedback on potential matching elements.

5.2 Weird Knocking Noise

The objective of this challenge is to analyze network data traffic using the Wireshark tool in order to identify a hidden message. Wireshark is frequently used in practice and is therefore an appropriate example to introduce to participants to network analysis which is also performed in undergraduate courses like data networks and IT security.

The description of the challenge for participants is as follows: “For several days, an unusual rhythmic knocking sound has been emanating from the neighboring office. I have elected to pursue this matter further and initiated a Wireshark capture of the network traffic, but the resulting data does not yield any insights. I would be grateful for your assistance.” Additionally, the aforementioned capture is provided to participants in the form of a PCAP file, which can be opened and analyzed in Wireshark.

A superficial examination of the network recording suggests that it contains only malformed DNS packets. Upon closer examination of the packet data, however, it becomes evident that Wireshark’s

Table 1: List of CampusQuest challenges.

Name	Difficulty	Category	Tags	Flag Type	Source
Hotel Where? (evidence search)	simple	Digital Forensics	Android, Forensics, Analysis	Static	https://cyberdefenders.org/blueteam-ctf-challenges/the-crime/
Puzzle Frenzy	simple	Digital Forensics	RDP, Cache, Riddle	Static	Own Development
GIF Puzzle (How to pronounce GIF)	medium	Digital Forensics	Riddle, GIF, QR-Codes	Static	https://ctftime.org/task/17415
Hidden Message (Imaged)	medium	Digital Forensics	Hex, Stegano, PNG, CRC	Static	https://ctftime.org/task/1924
Remote Password Manager	medium	Digital Forensics	RDP. RAM, Volatility	Static	https://ctftime.org/task/14640
Weird Knocking Noise	simple	Network Security	Morse-Code, Wireshark, PCAP	Static/ Dynamic	Own Development
Cupcakes	simple	Cryptology	Encryption	Static	https://ctftime.org/task/25405
Monoalphabetic Encryption	simple	Cryptology	Encryption, Analysis	Static	Cryptology Lecture at own University
Really Small Algorithm	simple	Cryptology	Encryption, RSA	Static	https://ctftime.org/task/11891
Paint it!	simple	Cryptology	Riddle, Stegano	Static	https://ctftime.org/task/1930
Unsafe Hotspot	difficult	Network Security	WLAN, Cracking, Encryption	Dynamic	Own Development

packet bytes pane contains information that is consistently represented by a single point or a single hyphen.

In conjunction with the designation of the challenge and the accompanying description, it is reasonable to assume that the concealed data may be represented by Morse code. To verify this hypothesis, the complete network traffic data can be displayed in Wireshark. To test this hypothesis, the selected packets are followed and the “UDP stream option” is selected, showing the expected dot and hyphen pattern, which then can be manually or automatically decoded using a website to obtain the flag.

To illustrate the modification of static flags to dynamic flags, a Python script was developed for the challenge “Weird Knocking Noise”. This script automatically creates PCAP files containing a freely selectable flag in Morse code. To this end, the Python library Scapy is employed, which enables the creation and processing of network packets in Python. When used in conjunction with the flag creation scripts, it is possible to generate a personalized or time-based challenge for each participant.

6 SUMMARY AND OUTLOOK

This paper presented CampusQuest, a platform for a continuous and physically present campus-based program on cybersecurity at a university. The target audience is primarily novices who are encouraged to engage with the subject of IT security. However, the platform can also be utilized by more experienced students and for other topics within the field of computer science or other academic disciplines. The platform facilitates the straightforward creation and management of challenges. It also enables the generation of personalized, dynamic flags to prevent the dissemination of solutions to challenges by simply exchanging the flags.

In order to test the functionality of the platform, a preliminary version of CampusQuest was created. This version includes a number of sample challenges, some of which were derived from existing events and some of which were developed anew. The physical aspect of the quest tasks was implemented through the use of 3D-printed entrance points with QR codes or CampusQuest boxes for the storage of small devices. These entrance points were designed to serve as a focal point, stimulating the curiosity of students and encouraging their participation in the quest.

The current status of the project is that initial challenges have been tested and deployed. Additional challenges, which are designed to build upon one another in a systematic manner, are currently being developed as part of final-year projects.

REFERENCES

Bmc-tools (2024). url: https://github.com/ANSSI-FR/bmc-tools (accessed on Oct 20, 2024).

BSI (2024). RdpCacheStitcher. url: https://github.com/BSI-Bund/RdpCacheStitcher/tree/main (accessed on Oct 20, 2024).

Chung, K. (2017). Live Lesson: Lowering the Barriers to Capture The Flag Administration and Participation. In: 2017 USENIX Workshop on Advances in Security Education (ASE 17). USENIX Association. url: https://www.usenix.org/conference/ase17/workshopprogram/presentation/chung (accessed on Oct 20, 2024).

Chung, K. (2024a). CTFD: What is capture the Flag? url: https://ctfd.io/whats-a-ctf/ (accessed on Oct 20, 2024).

Chung, K. (2024b). CTFd: The Easiest Capture The Flag Framework. url: https://ctfd.io/about/ (accessed on Oct 20, 2024).

Csikszentmihalyi, M. (1990). Flow: The Psychology of Optimal Experience. Harper Perennial. isbn: 9780060920432

CTFd (2024a). GitHub - CTFd/ctfcli: ctfcli is a tool to manage Capture The Flag events and challenges — github.com. url: https://github.com/CTFd/ctfcli (accessed on Oct 20, 2024).

CTFd (2024b). CTFd Exports | CTFd Docs - docs.ctfd.io. url: https://docs.ctfd.io/docs/exports/ctfd-exports/ (accessed on Oct 20, 2024).

Ctftime (2024). url: https://ctftime.org/ctf-wtf/ (accessed on Oct 20, 2024).

CyberDefenders (2024). CyberDefenders. url: https://cyberdefenders.org/blue-team-labs/plans/ (accessed on Oct 20, 2024).

CyberVista (2020). Capture the flag (CTF): A gamification of cybersecurity learning. url: https://certify.cybervista.net/capture-the-flag-agamification-of-cybersecurity-learning/ (accessed on Oct 20, 2024).

Deterding, S., Dixon, D., Khaled, R., Nacke, L. (2011). From game design elements to gamefulness. In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. Publisher Artur Lugmayr et al. ACM, 2011, pp. 9–15. isbn: 9781450308168. doi: 10.1145/2181037.2181040.

Diercks, J., Kupka, K. (2013). Recrutainment - Meaning, Influencing Factors and Definition (in German). In: Recrutainment. Publisher Diercks, J., Kupka, K. Springer-Gabler, 2013, pp. 1–18. isbn: 3658015691. doi: 10.1007/978-3-658-01570-1_1.

European Parliament (2023). The NIS2 Directive - A high common level of cybersecurity in the EU. url: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (accessed on Oct 20, 2024).

Gonzales-Scheller, P. (2013). The trending topic of gamification: what's behind this term? (in German). In: Recrutainment. Publisher Diercks, J., Kupka, K. Springer-Gabler, 2013, pp. 33–51. isbn: 3658015691. doi: 10.1007/978-3-658-01570-1_1.

Hacking Academy (2024). CTF-Hacking (in German). url: https://hacking-akademie.de/capture-the-flag-ctf-hacking/ (accessed on Oct 20, 2024).

HackTheBox (2024a). Hack The Box - Hacking-Labs. url: https://www.hackthebox.com/hacker/hacking-labs (accessed on Oct 20, 2024).

HackTheBox (2024b). HTB Academy. url: https://academy.hackthebox.com/preview/certifications (accessed on Oct 20, 2024).

Huawei (2024). Huawei Health App. url: https://consumer.huawei.com/de/mobileservices/health/ (accessed on Oct 20, 2024).

ICS2 (2023). Cybersecurity Workforce Study, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e (accessed on Oct 20, 2024)

Jacob, A., Teuteberg, F. (2017). Game-Based Learning, Serious Games, Business Games and Gamification - Application scenarios conducive to learning, insights gained and recommendations for action (in German). In: Gamification and Serious Games. Publishers Strahringer, S., Leyh, C. Edition HMD. Springer Fachmedien Wiesbaden, 2017, pp. 97–112. isbn: 978-3-658-16741-7. doi: 10.1007/978-3-658-16742-4_8.

Kahoot (2024). About Us. url: https://kahoot.com/company/ (accessed on Oct 20, 2024).

Kelly, S. (2019). What Is Python? In: Python, PyGame, and Raspberry Pi Game Development. Apress, 2019, pp. 5–9. isbn: 978-1-4842-4533-0. doi: 10.1007/978-1-4842-4533-0_2.

Kim, S., Song, K., Lockee, B., Burton, J. (2018). What is Gamification in Learning and Education? In: Gamification in Learning and Education. Publisher Kim S. et al. Springer International Publishing, 2018, pp. 25–38. isbn: 978-3-319-47282-9. doi: 10.1007/978-3-319-47283-6_4.

Luber, S., Schmitz, P (2020). What is a Blue Team? (in German). url: https://www.security-insider.de/was-ist-ein-blue-team-a-911741/ (accessed on Oct 20, 2024).

Mentimeter (2023). Annual Report 2023. url: https://storage.mfn.se/a/mentimeter/917e22f7-6165-4cfa-8c73-a01820d71255/mentimeter_annual-20report_2023-20-eng.pdf (accessed on Oct 20, 2024).

Microsoft (2021). Open Specifications: 3.1.1.1.1 Bitmap Caches. url: https://learn.microsoft.com/en-us/openspecs/windows_protocols/msrdpegdi/2bf92588-42bd-4527-8b3e-b90c56e292d2 (accessed on Oct 20, 2024).

Müller, H., Jahnke, J., Smith, D., Storey, M., Tilley, S., Wong, K. (2000). Reverse engineering. In: Proceedings of the Conference on The Future of Software Engineering. Publisher Finkelstein, A. ACM, 2000, pp. 47–60. isbn: 1581132530. doi: 10.1145/336512.336526.

Nike (2024). Nike Run Club. 2024. url: https://www.nike.com/de/nrc-app (accessed on Oct 20, 2024).

Ophie (2023). Hack The Box reaches 2 million platform members worldwide: Yet another great milestone for the #1 upskilling platform. url: https://www.hackthebox.com/blog/htb-two-million-platformmembers#:~:text=Hack%20The%20Box%20(HTB)%2C,globally%20across%20the%20HTB%20multiverse (accessed on Oct 20, 2024).

PentesterLab (2024). PentesterLab. url: https://pentesterlab.com/ (accessed on Oct 20, 2024).

PortSwigger (2024). PortSwigger WebSecurity Academy. url: https://portswigger.net/web-security (accessed on Oct 20, 2024).

Schindler, J. (2023). Survey: 71% of the IT skills shortage relates to cybersecurity (in German). url: https://news.sophos.com/dede/2023/12/05/umfrage-it-fachkraeftemangel-bezieht-sich-zu-71-auf-den-bereich-cybersecurity/ (accessed on Oct 20, 2024).

Statista Research Department (2023). The number of open positions for IT professionals in Germany up to 2023 (in German). url: https://de.statista.com/statistik/daten/studie/165928/umfrage/jahresvergleich-der-offenen-stellen-fuer-it-fachkraefte/ (accessed on Oct 20, 2024).

Toda, A., Pedro, H., Isotani, S. (2018). The Dark Side of Gamification: An Overview of Negative Effects of Gamification in Education. In: Higher Education for All. From Challenges to Novel Technology-Enhanced Solutions. Publishers Cristea A. et al. Vol. 832. Communications in Computer and Information Science. Springer International Publishing, 2018, pp. 143–156. isbn: 978-3-319-97933-5. doi: 10.1007/978-3-319-97934-29.

TryHackMe (2024). TryHackMe. url: https://tryhackme.com/ (accessed on Oct 20, 2024).