Expanding Horizons: The Evolving Landscape of Development Opportunities in Cybersecurity Training Platforms

Rebeka Tóth[1] and László Erdődi[2]

[1] University of Oslo, Norway
rebekat@ifi.uio.no
[2] University of Oslo,Norway
laszloe@ifi.uio.no

Abstract. In today's cybersecurity landscape, offensive security plays a vital role in fortifying systems by identifying vulnerabilities and potential attack vectors. Equally significant is the training of offensive security professionals. This study conducts a comprehensive comparative analysis of renowned offensive security training platforms: Hack The Box, TryHackMe, HackerOne, PicoCTF, and PortSwigger Academy. The goal is to evaluate these platforms across eight criteria, shedding light on their strengths and limitations, while also proposing potential enhancements to address existing gaps. The criteria encompass hints, ranking systems, flags, writeups, user feedback, knowledge domains, difficulty levels, and extensibility. By subjecting these platforms to this comprehensive evaluation, we gain invaluable insights into their individual advantages and areas necessitating improvement. A salient finding of the analysis is the absence of personalized learning pathways and adaptive training based on users' unique skills and cognitive patterns. To mitigate this gap, prospective offensive security training platforms could leverage machine learning algorithms to create customized learning experiences. By adopting user activity-driven methodologies, these platforms can tailor training content, challenges, and feedback to meet learners' distinct needs and skill levels. The outcomes of this study contribute to the advancement of offensive security training by outlining the features and attributes of a plausible future platform, grounded in the pivotal considerations necessary for the creation of a more comprehensive and efficient training ecosystem. By integrating personalized learning paths and harnessing the potential of machine learning, forthcoming platforms can provide tailored experiences that optimize learning outcomes and foster enhanced engagement.

Keywords: offensive security · training platforms · machine learning · personalized learning.

1 Introduction

The rise of the internet and digitization has brought great convenience to our lives, but it has also introduced risks and challenges in the realm of cybersecurity.

The rapid adoption of teleworking, online transactions, and virtual communication channels has led to an increase in cyber-attacks, posing significant threats to individuals, organizations, and society. Addressing these challenges is crucial, as cybersecurity awareness and education struggle to keep pace with the evolving digital landscape. Robust protective measures and fortified infrastructure are essential to mitigate cyber risks. However, the global shortage of IT professionals, particularly in security testing and vulnerability assessment, exacerbates the problem [1]. The growing demand for cybersecurity experts highlights the importance of cybersecurity education programs in training professionals with the necessary knowledge and skills. To meet the diverse competencies required in different cybersecurity specialties, an integrable framework and methodology are needed to provide a holistic and comprehensive approach to education while supporting sector-specific competency transfer.

1.1 Offensive security

Offensive security, also often called ethical hacking, significantly strengthens overall cybersecurity. Penetration testing, widely adopted by organizations, aims to unveil system vulnerabilities proactively to fortify information systems. However, if not executed precisely, it may exacerbate issues rather than mitigating them [7]. Through controlled attempts to exploit vulnerabilities, it pinpoints system weaknesses, facilitating timely remediation before malicious exploitation occurs. The term vulnerability is defined by cybersecurity agencies in several ways. However, there is minimal variation between them. For example, the National Institute of Standards and Technology (hereafter NIST) defines vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [9]. Ethical hacking stands in stark contrast to the criminal activities associated with black-hat hacking. Ethical hacking is conducted professionally, typically by reputable companies hired to rigorously test systems while adhering to the highest ethical standards, including being carried out with consent, conducted by experts, by security-cleared consultants, in accordance with the legislation in force, and with full transparency [8].This proactive stance empowers organizations to assess security, detect potential entry points, and bolster defenses. The approach offers multifaceted advantages. It mirrors real-world attacks, deepening vulnerability comprehension and enhancing defense readiness. It also identifies and rectifies infrastructure flaws, from misconfigurations to outdated software. By scrutinizing detection and response mechanisms, offensive security elevates incident response capabilities, minimizing potential damage. Moreover, it keeps organizations ahead of cyber threats by staying attuned to the latest tactics, allowing proactive adaptation of defenses. In essence, offensive security is a preemptive strategy that reinforces defense, optimizes incident response, and ensures robust cybersecurity in a swiftly evolving digital realm [2].

The field of cybersecurity changes rapidly consequently training, and studying is a continuous and steady process for all security professionals. Despite

formal education, cybersecurity competitions are exceedingly popular and effective methods of learning in the field of cybersecurity. There are three main types of cybersecurity competitions: technical, non- technical and mixed. The technical competitions are called Capture the Flags (CTF) and require very thorough technical knowledge. Non-technical competitions are often called strategic challenges, however there is a common name for this type of competitions as for the CTFs and require legal, media, reporting and high-level cybersecurity knowledge. Mixed competitions usually require both technical and non-technical skills. CTF competitions, an increasingly favored approach for honing security skills, engage participants in security-themed challenges to test their prowess [3]. In these competitive computer security events, individuals or teams vie for the highest score by capturing flags, typically encoded as random strings or embedded data fragments within challenges [4]. These challenges exhibit diverse formats, encompassing linear puzzles, as well as offensive and defensive hacking scenarios like forensics or web application hacking [5]. CTF competitions and games often touch on many aspects of information security such as steganography, malware analysis, mobile security or even information technology auditing. Consequently, teams should have strong skills, broad knowledge, and experience in all these fields [6].

2 Background

2.1 Related literature

Araújo, L., et al. delve into evaluating cybersecurity Capture the Flag (CTF) platforms, including Hack The Box and TryHackMe, in terms of their efficacy in bolstering cybersecurity skills. Their study undertakes an in-depth analysis of CTF platforms, extracting essential components for their application as e-Learning tools in higher education. Through a systematic comparative and experimental study involving interviews with computer science undergraduates, the researchers gather insights on the platforms' attributes. The participants' perspectives contribute to assessing the effectiveness of these CTF platforms and their relevance to cybersecurity education [10].

Kancherla, A., et al. spotlight the role of HackTheBox and Capture The Flag (CTF) style challenges in cybersecurity education. The research probes the impact of these challenges on students' practical knowledge and skills in cybersecurity, addressing design, pedagogy, assessment methods, and students' engagement. By delving into students' experiences, the study provides valuable insights into the incorporation of hands-on activities, enhancing cybersecurity education's effectiveness. This research offers a window into innovative and experiential learning methods, promoting effective teaching practices in cybersecurity [11].

Shukla, R., & Rao, M. N. focus on the evaluation of TryHackMe's virtual cybersecurity labs. The research assesses the platform's features, functionality, and impact on hands-on training and skill development. By analyzing the range of topics, complexity of challenges, user interface, and overall experience, the study

aims to provide educators and learners with insights into the strengths and weaknesses of TryHackMe as a virtual cybersecurity lab platform. This examination aids informed decision-making for cybersecurity training and education purposes [12].

2.2 New horizons

While the aforementioned publications provide valuable insights into existing cybersecurity platforms such as Hack The Box and TryHackMe, there are certain aspects that they may not fully address. One area of improvement is the need for platforms to continuously evolve and offer more advanced features to keep pace with the rapidly changing cybersecurity landscape. Additionally, these publications do not extensively discuss the possibilities of creating a future platform that can adapt to individual personality traits and learning styles. A more effective platform would provide a tailored training path for each individual based on their unique skills and ways of thinking. Furthermore, while the publications may identify weaknesses in the current platforms, they may not provide concrete solutions or recommendations for addressing these weaknesses. Future research could focus on proposing innovative approaches or enhancements to overcome the limitations of existing platforms and improve the overall learning experience for cybersecurity enthusiasts. Based on the above mentioned, research will explore the possibilities of a new future cyber security training platform.

3 Educational platforms

In cybersecurity education, students often practice red-teaming, conducting penetration tests to assess system resilience against unauthorized access which offers firsthand insights into safeguarding sensitive data, evaluating security measures, and understanding real-world threats. The most popular platforms like Hack The Box (HTB) with a user base of 2 million, TryHackMe (THM) with also 2 million registered users, HackerOne (H1) with over a million, PicoCTF with eighteen thousands, and PortSwigger Web Academy with one million users, nurture aspiring cybersecurity professionals. They simulate real-world hacking scenarios, enabling hands-on experience in vulnerability identification, exploitation, and countermeasures. Within ethical boundaries, these platforms provide safe spaces for responsible exploration. They're vital tools in cultivating the next cybersecurity generation, equipping them to protect digital assets against malicious activities.

Hack The Box offers a comprehensive virtual lab environment, featuring a wide range of realistic scenarios for hands-on experience in multiple security domains. Additionally, it provides an enterprise platform with customizable content for employee training and candidate evaluation. HTB Academy offers guided learning paths with explanatory background for various security topics. Conversely, TryHackMe emphasizes user-friendly interfaces and accessibility, catering to both beginners and experienced users. Its guided learning paths and interactive challenges enhance the learning process. HackerOne primarily serves as

a bug bounty platform, linking security researchers with organizations for ethical hacking collaborations. PicoCTF focuses on educational purposes, offering gamified challenges and tutorials in diverse cybersecurity topics. PortSwigger Academy specializes in web application security training, concentrating on the OWASP Top 10 vulnerabilities with hands-on interactive labs. Platform evaluations consider criteria such as challenge diversity and quality, effective hint systems, ranking mechanisms, teaching materials availability, and write-ups for post-challenge learning.

3.1 Methodology

The above-mentioned teaching platforms are very similar and all of them offer free and premium challenges, however they may vary in certain parts such as content, design or approaches. They all offer comprehensive training resources, including tutorials, challenges, and interactive exercises, to cater to learners of varying skill levels. This accessibility and scalability allow individuals to acquire practical cybersecurity knowledge and develop critical thinking, problem-solving, and teamwork skills, which are invaluable in combating the ever-evolving landscape of cyberthreats.

For this research, the most popular CTF style learning platforms were selected. We have identified and employed a set of carefully chosen criteria to conduct a comprehensive analysis and subsequent ranking of the selected platforms. The evaluation base don the below criteria:

1. Hints: Evaluate the availability and effectiveness of hints or guidance provided during challenges or exercises.
2. Ranking system: Examine the structure and effectiveness of the ranking system employed by each platform to encourage and reward user performance.
3. Flags: Analyze the flag management system, including the quality and variety of flags provided in the challenges.
4. Writeups: Assess the availability and quality of writeups for learning purposes, which provide detailed explanations and solutions for completed challenges.
5. User feedback: Consider the feedback and reviews from users to gain insights into the user experience and satisfaction.
6. Fields of knowledge: Analyze the breadth and depth of cybersecurity topics covered by each platform, ensuring they align with the desired learning objectives.
7. Difficulty levels: Evaluate the range and progression of difficulty levels offered by the challenges to cater to different skill levels and learning needs.
8. Extensibility and penalization: Consider the extensibility of the platform and customization of the platform to tailor it to the users' needs, integration options, or the ability to create custom challenges or content.

By considering these categories, a comprehensive and detailed comparison can be made to assess the strengths and weaknesses of each platform in relation to the desired learning outcomes and user preferences.

3.2 Evaluation

Hints Hints are indispensable tools in the realm of offensive security training, offering learners essential guidance while nurturing independent problem-solving skills. The hint systems adopted by various platforms play a pivotal role in shaping the overall learning experience. For instance, Hack The Box's academy section features a distinct hint mechanism that provides users with progressive hints, empowering them to navigate challenges while ensuring they arrive at solutions through their efforts. A similar approach is employed by TryHackMe, where incremental hints are aligned with challenge difficulty levels, aiding learners in overcoming obstacles step by step. HackerOne, functioning as a bug bounty platform, fosters experiential learning by promoting collaboration between security researchers and organizations. This practice offers learners real-world insights and guidance during assessments, resulting in a dynamic learning curve. PicoCTF, designed for educational purposes, adopts a comprehensive model by offering both tutorials and contextual hints tailored to each challenge. This not only aids in arriving at solutions but also deepens the understanding of fundamental concepts. PortSwigger Academy, specializing in web security, provides learners with step-by-step assistance within interactive labs, enabling them to identify and exploit web application vulnerabilities effectively. Evaluating hint systems encompasses factors such as clarity, relevance, and balance. Effective hints should provide enough information to drive learners forward while fostering independent analytical skills. The availability and quality of hints significantly contribute to learners' ability to conquer challenges and develop problem-solving acumen. The diverse hint approaches across these platforms cater to learners with varying proficiency levels. By delving into the nuances of hint systems, learners, practitioners, and developers can glean insights into effective guidance strategies. This analysis not only aids in refining existing platforms but also guides the development of future ones that prioritize enhanced support and guidance, thus enriching the landscape of offensive security education.

Table 1. Evaluation for hints.

Hints	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Traits	No official hints, unofficial forum comments	Hard coded, static hints	No inserted direct hints	Contextual hard coded hints	Hard coded, static hints

Ranking system Hack The Box employs a robust ranking system centered around "ranks" and "points." As users successfully conquer challenges, they earn points that translate into increased ranks, motivating a continuous pursuit of higher achievements. This mechanism propels users through varying difficulty levels and ignites competition for higher positions on the leaderboard,

offering a palpable sense of accomplishment. TryHackMe adopts a badge-centric ranking approach, awarding badges for completing tasks or reaching milestones. These badges signify users' competence in different cybersecurity domains, serving as visible representations of their accomplishments. This system encourages exploration of diverse learning paths and showcases expertise within the TryHackMe community. HackerOne, operating as a bug bounty platform, relies on a reputation-based ranking system. Users accumulate reputation points based on the caliber and impact of their vulnerability discoveries. This structure promotes robust competition among security researchers, spotlighting their expertise and credibility through reputation scores. PicoCTF, an educational platform, implements a points-based ranking system tied to challenge completion and flag capture. The challenges' difficulty level correlates with the points awarded, motivating users to tackle progressively intricate tasks and bolster their cybersecurity proficiency. PortSwigger Academy, renowned for its web security training, lacks a formal ranking system. However, it presents a comprehensive learning trajectory enabling users to trace their progress and amass expertise in web application security. While not centered on competition, PortSwigger Academy concentrates on advancing knowledge and skills in the realm of web security. Overall, these platforms' ranking systems encourages and honor user accomplishments. They foster a sense of achievement, recognition, and positive rivalry, propelling users to refine their competencies, engage with advanced challenges, and contribute actively to the cybersecurity realm.

Table 2. Evaluation for ranking system.

Ranking	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Assessment	Robust ranks and points system	Badge-based system	Reputation-based system	Point-based system	N/A (No formal ranking system)
Details	Earn points by completing challenges, rank increase on the leaderboard, motivates to progress and compete	Earn badges for achievements, proficiency in different domains, encourages exploration of different paths	Earn reputation based on findings, report accuracy. Showcases expertise and credibility	Earn points for challenge completion and flag captures. Encourages tackling challenging tasks	Focuses on learning path and skill development within web security

Flags Hack The Box offers a broad spectrum of challenges, each featuring unique and specific flags that encapsulate various dimensions of cybersecurity. These flags are meticulously crafted to align with intended learning objectives, ensuring their characteristics and quality. The complexity of these flags stimulates com-

prehensive skill growth, demanding an in-depth grasp of diverse techniques and methodologies. TryHackMe adopts a flag system closely tailored to each room's learning paths and goals. Balancing beginner-friendly flags that emphasize foundational concepts and advanced flags requiring intricate problem-solving, the platform covers a wide spectrum of user proficiencies. This array enables users to progressively explore diverse cybersecurity domains, enriching their knowledge and expertise. HackerOne, functioning as a bug bounty platform, employs a distinctive approach. Instead of predefined flags, users are prompted to pinpoint and report real-world application vulnerabilities. The successful identification and reporting of these vulnerabilities act as the equivalent of flags, evaluated based on their impact and validity. This emphasizes the quality and significance of identified vulnerabilities over predefined flags. PicoCTF furnishes challenges with flags spanning an array of cybersecurity themes such as web application security, cryptography, and reverse engineering. These flags evaluate users' grasp and application of pertinent concepts within each challenge category. The platform ensures a balanced mix of flags catering to various difficulty tiers, guaranteeing an engaging and incremental learning journey. PortSwigger Academy strategically embeds flags within its web security training challenges to validate users' comprehension of web vulnerabilities and their exploitation. These flags simulate real-world scenarios, encouraging users to adopt an attacker's mindset. The assortment of flags corresponds to distinct web vulnerability types and techniques, enabling users to master various offensive cybersecurity aspects. Overall, these platforms' flag management systems prioritize high-quality flags aligned with learning objectives and challenge difficulty levels. These flags stimulate comprehensive skill development, foster creative problem-solving, and allow users to showcase their mastery of diverse offensive cybersecurity elements.

Table 3. Evaluation for flags.

Flags	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Assessment	Unique, specific, and representative of objectives	Aligned with learning paths and objectives	Real-world vulnerabilities reported by users	Cover diverse cybersecurity topics	Validate understanding of web vulnerabilities
Details	Diverse challenges,various aspects, requiring deep understanding	Balanced fundamental and advanced concepts enhancing knowledge and expertise progressively	Identifying and reporting real-world bugs, significance and impact of vulnerabilities	Wide spectrum of topics, varying difficulty levels, engaging and progressive learning	Real-world scenarios and exploit techniques, promote comprehensive skill development

Writeups Hack The Box stands out with its robust collection of user-contributed writeups, forming an educational treasure trove. These writeups serve as comprehensive guides, detailing the intricate methodologies, techniques, and tools employed to conquer challenges. A hallmark of community collaboration, they cater to diverse skill levels, building a reservoir of knowledge. The platform actively encourages a spirit of knowledge sharing, resulting in well-crafted explanations that foster a deep understanding among users. Similarly, TryHackMe bolsters its learning experience through user-generated writeups. These walkthroughs offer users the chance to dissect others' approaches and experiences, aiding in the development of effective problem-solving strategies. Although the quality of TryHackMe's writeups varies, the platform boasts numerous meticulously crafted and informative resources.

In contrast, HackerOne's emphasis on real-world applicability steers it away from traditional writeups. Instead, the platform emphasizes detailed vulnerability reports as learning materials, aligning closely with practical industry demands. However, it does provide guidance on constructing impactful reports, an educational avenue for those aspiring to delve into vulnerability analysis and bug hunting. PicoCTF, catering to educational needs, presents insightful writeups that deconstruct challenges, guiding users through the thought processes and methodologies employed to tackle them. These well-structured writeups offer a deep dive into the concepts underlying each challenge.

In the field of web security, PortSwigger Academy delivers comprehensive explanations and solutions for its interactive labs, bridging the gap where dedicated writeups are absent. While not traditional writeups, these resources are designed to guide users through the identification and mitigation of web vulnerabilities, furnishing learners with a solid grasp of web security principles. Although writeup availability and quality vary across platforms, they collectively represent valuable assets for learners. These educational materials elucidate the intricate landscape of offensive security techniques, contributing significantly to users' grasp of cybersecurity intricacies.

Table 4. Evaluation for writeups.

Writeups	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Assessment	Tutorials, walk-throughs, documentation	Detailed learning paths, written and video tutorials	Vulnerability disclosure guidelines, bug hunting tips	Comprehensive material, tutorials, explanations	Interactive labs, tutorials, documentation
Details	User made video and written guides	Official and unofficial user made written and video guides	Practical, step-by-step bug bounty reports	Clear explanations and resources for further exploration	Thorough, engaging guides

User feedback Hack The Box has a vibrant community of users who actively provide feedback and reviews on challenges, features, and overall platform experience. Users often share their thoughts on the difficulty levels, quality of challenges, and the effectiveness of the learning materials. This feedback can provide valuable insights into the strengths and areas for improvement of the platform. TryHackMe encourages users to provide feedback through various channels, including forums, chat rooms, and direct interactions with the platform's support team. Users share their experiences, offer suggestions for improvements, and discuss the platform's content and features. This feedback helps shape the platform's development and aids in enhancing the user experience. HackerOne, being a bug bounty platform, collects feedback from security researchers and organizations engaging in vulnerability assessment and reporting. Researchers share their experiences with the platform's processes, communication, and overall satisfaction. Organizations provide feedback on the effectiveness of the platform in addressing their security needs. This feedback contributes to the continuous improvement of the platform's functionality and services. PicoCTF receives feedback from its user community, consisting primarily of students and educators. Users share their experiences with the challenges, educational resources, and the overall learning environment. This feedback helps the platform in refining its content, addressing any usability issues, and aligning the platform with the educational goals of its target audience. PortSwigger Academy gathers feedback from users regarding their experiences with the web security training and educational resources provided. Users provide insights into the clarity of instructions, the effectiveness of labs and exercises, and the overall usefulness of the platform in enhancing their web security skills. This feedback contributes to the continuous improvement of the platform's content and delivery.

By considering user feedback and reviews, researchers can gain valuable insights into the strengths, weaknesses, and user satisfaction of offensive security training platforms. This feedback can aid in making informed decisions about the suitability of these platforms for specific training objectives and user preferences.

Table 5. Evaluation for user feedback.

Hints	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Assessment	Reviews on challenges, difficulty levels	Share suggestions, experiences	From researchers, organizations on processes, overall satisfaction	Share experiences, provide insights	On clarity of instructions, effectiveness of labs, usefulness
Details	Highlight platform's strengths and weaknesses	Shapes platform development, enhances the experience	Improvement of functionality and services	Refine content, address usability issues, align with goals	Improvement of content and delivery

Fields of knowledge Hack The Box presents an extensive array of challenges spanning diverse cybersecurity domains, encompassing network security, cryptography, reverse engineering, web application security, and more. These challenges cater to both novice and advanced users, offering varying difficulty levels. This versatility empowers learners to delve into multiple facets of cybersecurity, progressively honing their expertise. Conversely, TryHackMe adopts a practical approach by furnishing users with immersive learning environments termed "rooms." These encompass a broad spectrum of cybersecurity topics, including penetration testing, network security, and web application security. Structured learning paths and guided missions within the platform enable users to methodically pursue their learning objectives. HackerOne, distinct as a bug bounty platform, directs its focus towards authentic vulnerabilities and hands-on security evaluations. This immersion in real-world scenarios allows participants to engage in bug bounty programs for diverse organizations. This pragmatic experience equips learners to apply their knowledge in identifying and rectifying vulnerabilities within actual systems, cultivating practical prowess. Tailored for educational purposes, PicoCTF delivers gamified challenges spanning cryptography, binary exploitation, forensics, and more. This educational gamification offers a comprehensive learning venture, ensuring learners' exposure to an extensive scope of cybersecurity domains. Concentrating on web application security, PortSwigger Academy offers intensive training in this domain. Its comprehensive curriculum spans secure coding practices, web vulnerabilities, and advanced techniques for identifying and countering web-based security issues. By analyzing the breadth and depth of cybersecurity topics covered by each platform,it can be concluded that all platforms provides the necessary coverage of topics and enables users to acquire knowledge and skills in the specific areas of cybersecurity that they wish to focus on.

Table 6. Evaluation for the provided areas of knowledge.

Fields	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Web Application	Yes	Yes	No	Yes	Yes
Network Security	Yes	Yes	Yes	No	No
Cryptography	Yes	Yes	No	Yes	No
Reverse engineering	Yes	Yes	No	Yes	No
Penetration testing	Yes	Yes	Yes	No	No
Bug Bounties	No	No	Yes	No	No
Forensics	Yes	Yes	No	Yes	No
Secure Coding	No	No	No	No	Yes
Gamified	Yes	Yes	No	Yes	No

Difficulty levels Hack The Box showcases an extensive array of challenges tailored to varying difficulty levels, accommodating users with diverse levels of expertise. This inclusive design empowers learners to select challenges aligned with their competencies, enabling gradual advancement to more intricate tasks. By steadily escalating the complexity of challenges, the platform ensures a seamless learning curve, allowing users to progressively enhance their skills. TryHackMe mirrors this approach by furnishing challenges and rooms catering to distinct proficiency tiers. From entry-level content for cybersecurity novices to sophisticated challenges for seasoned practitioners, the platform supports a learning continuum. Users can methodically select challenges matching their skill levels, promoting a seamless learning journey. HackerOne adopts a real-world approach, presenting challenges that span different difficulty levels, contingent on the intricacy of vulnerabilities and the level of security measures. As users gain expertise and demonstrate their capabilities, they gain access to more demanding bug bounty programs, fostering an environment of continual skill development. PicoCTF specializes in educational challenges, offering a spectrum of difficulty levels. This thoughtful progression equips learners to begin with foundational concepts, gradually advancing to more complicated subjects. This step-by-step approach ensures learners systematically cultivate their skills, bolstering confidence as they tackle progressively challenging scenarios. PortSwigger Academy hones in on web application security with its series of training modules and challenges. The platform orchestrates a coherent learning trajectory, covering rudimentary concepts and gradually integrating sophisticated techniques. Users can seamlessly navigate between modules, ensuring a structured improvement in their comprehension of web application security.

Through an assessment of the diversity and progression of difficulty levels encompassed by challenges on these platforms, researchers can gauge their appropriateness for distinct skill levels and learning requirements. This diversity in difficulty levels ensures learners of varying proficiencies can continually enhance their offensive security skills and knowledge.

Table 7. Evaluation for difficulty levels.

Levels	**HTB**	**THM**	**H1**	**PicoCTF**	**PortSwigger**
Beginner	Yes	Yes	Yes	Yes	Yes
Intermediate	Yes	Yes	Yes	Yes	Yes
Advanced	Yes	Yes	Yes	Yes	Yes
Gradual progression	Yes	Yes	No	Yes	Yes

Extensibility and penalization A highly extensible platform offers users the ability to adapt the training environment to their specific needs, integrate with other tools and systems, and contribute to the platform's growth and enrichment.

Hack The Box, known for its dynamic ecosystem, provides a highly extensible platform that enables users to not only engage with the existing challenges but also contribute to its expansion. This extensibility encourages users to devise innovative challenges, enriching the platform and fostering a collaborative environment. TryHackMe follows suit by allowing users to create their own teaching content or learning environments, making the platform remarkably adaptable. This feature permits trainers to curate content aligned with specific learning objectives, ensuring a personalized training experience. Additionally, the platform encourages integration with external tools, enhancing the versatility of the learning process. HackerOne, being a bug bounty platform, embodies extensibility through its collaboration with security researchers. This collaboration results in the identification of real-world vulnerabilities, contributing to the platform's ongoing development. The bug bounty framework ensures continuous enhancement and keeps the platform adaptable to emerging cyberthreats. PicoCTF champions extensibility by nurturing a community of educators and learners who can contribute challenges and educational content. This engagement encourages the platform's growth and diversification, allowing a wide range of topics to be covered in the challenges. PortSwigger Academy, specializing in web application security, supports extensibility by providing a framework for users to develop their own security labs and challenges. This feature not only enriches the learning experience but also allows users to engage in hands-on experimentation. The extensibility of these platforms resonates with the principles of active learning and customization, empowering users to adapt their training journeys. By fostering collaboration, supporting tool integration, and encouraging content contribution, these platforms create a progressive approach to offensive security education.

4 What would the future platform look like?

After conducting a thorough analysis, it can be concluded that all the examined platforms offer a comprehensive and hands-on learning environment, complemented by various personalization options and a skill matrix that tracks progress based on the types and categories of challenges completed by the user. Offensive security requires a well rounded set of skills which includes but not limited to the following: information gathering, open-source intelligence, network and infrastructure security, web application security, wireless security, cryptography, exploit development, mobile security, reverse engineering, physical security, operating system security, cloud security.

As mentioned above these platforms provide personalization to some instinct such as choosing the desired skill set that the user would like to learn, however the existing platforms only provide a one-size fits all, static learning path. A future platform with machine learning-based approach holds tremendous potential such as a fully personalized skill and ability based learning path generation. A platform where users would have the ability and freedom to choose their desired

learning path that would adapt to their personal needs and skills include the below characteristics:

Detection of strength and weaknesses: The learning platform employs advanced algorithms to intelligently analyze user interactions, patterns, and successful outcomes. By understanding the approaches that lead to successful solutions, the platform determines the users' areas of strength. This information is then utilized to curate challenges that align with their established expertise, ensuring that users engage with content that builds upon their existing skills. As users demonstrate competence, the platform continually refines its understanding of their strengths, contributing to an increasingly personalized learning experience. The platform would also discern areas where the users may have limitations and providing simplified tasks or incremental steps for improvement.

Dynamic hints: Rather than offering static hints that are hard coded for all users, the platform integrates a dynamic hint system. These hints adapt in real-time based on users' actions and the context of their challenge-solving process. By analyzing the methods users attempt and the steps they take, the platform intelligently generates hints tailored to their individual progress. This approach not only fosters self-directed learning but also ensures that users receive guidance that aligns with their specific problems and thought processes.

Automatic challenge generation: The platform harnesses the power of automation to generate challenges tailored to users' learning needs. Drawing insights from user preferences, strengths, and areas of improvement, it crafts challenges that precisely match their requirements. Furthermore, as new vulnerabilities emerge everyday, the platform proactively adapts by generating challenges that mirror these newly surfaced threats. This feature reduces the administrative burden of challenge creation and ensures that users constantly engage with relevant, up-to-date content.

Performance based difficulty level increase: Adaptivity is a cornerstone of the platform's approach to challenge difficulty. By continuously monitoring users' performance and progress, the platform dynamically adjusts the complexity of challenges they encounter. As users achieve milestones and demonstrate mastery, the platform incrementally raises the difficulty level to maintain a balance between challenge and growth. This personalized approach to challenge progression ensures that users are consistently challenged at an appropriate level, optimizing their learning journey.

Personalized learning path: The learning path on the platform is tailored to the individual journey of each user. Utilizing data on users' preferences, learning history, and areas requiring improvement, the platform creates a unique roadmap. This roadmap guides users through challenges, modules, and resources that align with their specific goals and learning pace. By adapting content and experiences to users' evolving needs, the platform ensures that every user's learning path is optimally suited to their development as an offensive security professional.

This platform blends machine learning and user-centric design to create a dynamic and adaptive learning environment for offensive security professionals.

On this platform a user could choose any offensive security topic and skill set such as web penetration testing. Upon selection, the platform would intelligently generate a personalized learning path tailored to the chosen domain, however at first without any previous learning logs for the current user, the learning path would only be a generalized path. Once a user starts solving challenges the machine learning algorithm would immediately start tailoring the learning path based on the students mistakes, weakness, strength and pace of learning

The learning platform's curriculum would be thoughtfully designed to encompass a range of critical topics in offensive security, covering essential aspects such as the OWASP Top 10, common vulnerabilities, web frameworks, and the utilization of crucial tools like Burp Suite, Nessus and other top rated offensive security tools. However, the true power of machine learning lies in its capacity to actively monitor and adapt to the individual user's actions and performance, thereby crafting a truly personalized learning experience. As the machine learning algorithm closely observes the user's activities and achievements, it excels at identifying areas of vulnerability and weakness. It capitalizes on this insight by generating challenges tailored to specifically target these identified weak points. In doing so, it goes beyond merely recognizing general areas of weakness, diving into a more granular exploration of specific cybersecurity topics. For instance, if a user struggles with web application security or a nuanced vulnerability like SQL injection, the machine learning algorithm delves deeply into these subjects. In the context of SQL injection, the platform's machine learning component employs a sophisticated approach. It analyzes the user's actions, techniques, and performance to accurately pinpoint the precise type of SQL injection vulnerability that poses a challenge to the user. Furthermore, it identifies the most relevant and effective exploitation methods associated with this vulnerability. This meticulous level of scrutiny ensures that users receive challenges that are highly targeted, addressing their specific weaknesses with pinpoint accuracy. The ultimate aim is to facilitate an immersive and comprehensive learning experience for offensive security practitioners. By focusing on these specific aspects, the platform offers a deeply tailored journey that enables practitioners to attain in-depth knowledge and expertise in the exact areas that warrant improvement. This approach not only ensures that users can address their weaknesses effectively but also propels them towards achieving mastery in the facets of offensive security that require attention. In sum, the learning platform leverages machine learning to deliver an educational experience that is unparalleled in its precision, adaptability, and personalization, resulting in a profoundly effective learning path for offensive security professionals.

5 Summary

A machine learning-based offensive security learning platform holds immense promise for the future. By offering personalized learning paths, adaptive challenges, dynamic hints, and comprehensive progress reports, such a platform

would revolutionize the learning experience and empower individuals to enhance their offensive security skills effectively.

The learning platform would provide a comprehensive report, highlighting the user's strengths and weaknesses based on their performance and progression. To enhance the learning experience, the machine learning algorithm would dynamically generate hints rather than relying on predetermined solutions. These hints would be tailored to the user's specific activity and problem-solving approach, ensuring personalized guidance that fosters skill development and critical thinking. Furthermore, the platform would simulate real-world scenarios. For instance, if a user successfully completes a simulated web application penetration test by discovering high and critical-level vulnerabilities, the machine learning algorithm would adapt by presenting challenges that focus on low, medium, and informational-level vulnerabilities. This approach would enable users to continuously hone their skills and tackle a diverse range of security challenges.

References

1. Leaser, David: The demand for cybersecurity professionals is outstripping the supply of skilled workers. Retrieved from International Business Machines, https://ibm.co/2Sd3K3h Last accessed 10 May 20223
2. Weaver, N.: Offensive Cybersecurity: A Practical Guide to Hacking and Penetration Testing. Packt Publishing. (2019)
3. Švábenský, V., et al.: Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security, 102, 102154. (2021)
4. European Union Agency for Cybersecurity: Capture-The-Flag Competitions: all you ever wanted to know! https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know. Last accessed 10 May 20223
5. Werther et. al.: Experiences In Cybersecurity Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise.
6. Kevin CHUNG: Recruiting and Teaching with Capture the Flags, https://blog.ctfd.io/recruiting-and-teaching- with-capture-the-flags/. Last accessed 27 May 2023
7. Farkhod et. al.: Methodology for Penetration Testing. International Journal of Grid and Distributed Computing Vol.2, No.2, June 2009.
8. Mitnick, K. D., & Simon, W. L.: The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. Wiley. (2005)
9. National Institute of Standards and Technology (NIST) Computer Security Resource Center: Glossary – Vulnerability, https://csrc.nist.gov/glossary/term/vulnerability. Last accessed 10 May 20223
10. Araújo, L., et al.: Evaluating Cybersecurity Capture the Flag Platforms. In Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6. (2020)
11. Kancherla, A., et al.: HackTheBox and Capture The Flag (CTF) Style Challenges in Cybersecurity Education. In Proceedings of the 2020 ACM Southeast Conference (ACMSE), pp. 1-6.
12. Shukla, R., & Rao, M. N.: An Analysis of TryHackMe Virtual Cyber Security Labs. International Journal of Advanced Computer Science and Applications, 11(1), 230-238. (2020)