Ethical hacking skills development through the PentestHUB platform

Alla D. Pinchuk, Roman S. Odarchenko and Oleh O. Polihenko

National Aviation University, 1 Liubomyra Huzara Ave., Kyiv, 03058, Ukraine

Abstract

The development of ethical hacking skills has become a crucial component of modern cybersecurity education. This paper introduces PentestHUB, an interactive platform that was developed to bridge the gap between academic curricula and real-world ethical hacking practice, enhancing learners problem-solving and ethical hacking skills. The comparison of existing solutions such as DVWA, Badstore, Hackxor and HackThisSite allowed to identify key limitations that should be improved. The PentestHUB addresses these key limitations like outdated vulnerabilities, limited coverage of modern standards (OWASP Top 10, OWASP ASVS, OWASP API Security Top 10, MITRE CWE), and insufficient extensibility. The platform offers scenario-based challenges, supplemented by a unique code-analysis feature that prompts learners to identify and remediate vulnerabilities. The PentestHUB's scalable, customizable design supports various difficulty levels, making it suitable for a wide range of educational contexts. This paper outlines the conceptual framework, technical implementation, and educational rationale of PentestHUB, underscoring its potential to strengthen university-level cybersecurity programs and foster advanced ethical hacking competencies.

Keywords

ethical hacking, penetration testing, skills development, educational platform, OWASP

1. Introduction

In recent years, the cyberthreat landscape, as well as the entire cyberspace, has significantly changed. Cyberattacks have become more sophisticated by using cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), etc. to bypass security measures. To protect our IT infrastructure from all these cyber threats, we need to test its security. Here is a need to use the same tools and approaches as real cyberthreat actors to assess the level of cybersecurity. In other words, it is necessary to use ethical hacking approaches. The development of ethical hacking skills has become a cornerstone of modern cybersecurity education, necessitating structured and comprehensive training programs within higher educational institutions (HEIs).

However, there remains a significant gap between theoretical knowledge imparted in traditional academic educational programs and the practical expertise required to apply this knowledge in real-world situations. Many universities focus predominantly on theoretical concepts, often due to the absence of their own custom tools and platforms that can bridge this divide. Without hands-on experience, students may struggle to develop the problem-solving abilities and technical competencies required for effective ethical hacking.

Indeed, on that count, it is vital that simulation-based online learning platforms are used by the teaching staff in cybersecurity educational programs. Such platforms allow students to apply their knowledge in controlled situations. PentestHUB was created to fill this gap, thus providing a practical aspect and structured acquisition of ethical hacking skills. This platform focuses on web application security, consisting of challenges based on OWASP Top 10 web application vulnerabilities, OWASP ASVS, OWASP API Security Top 10, etc. The developed PentestHUB platform provides a comprehensive

STEM@ICon-MaSTEd 2025: 4th Yurii Ramskyi STE(A)M Workshop co-located with XVII International Conference on Mathematics, Science and Technology Education, May 14, 2025, Ternopil, Ukraine

alla.pinchuk@kai.edu.ua (A. D. Pinchuk); roman.odarchenko@npp.kai.edu.ua (R. S. Odarchenko); o.poligenko@ukr.net (O. O. Polihenko)

0000-0003-3567-0445 (A. D. Pinchuk); 0000-0003-3567-0445 (R. S. Odarchenko); 0000-0002-2427-4976 (O. O. Polihenko)

framework for students to enhance their practical abilities, fostering both technical proficiency and a deeper understanding of cybersecurity principles, in particular web application security.

2. Literature review

The integration of ethical hacking into cybersecurity education has gained significant attention in recent years, as it bridges the gap between theoretical instruction and practical application [1]. Various studies underscore the importance of equipping students with hands-on experience to effectively address the complexities of modern cyberthreats. This section reviews key works that highlight the role of simulation-based platforms, ethical hacking pedagogy, and innovative teaching methods in advancing cybersecurity education.

Hartley [2] analyzed the foundational role of ethical hacking as a pedagogical method in higher education. The study emphasized the importance of teaching students to approach security challenges with the mindset of a hacker to understand vulnerabilities and preemptively secure systems. A notable highlight was the importance of combining technical skills with ethical considerations, ensuring students are trained to act responsibly.

The study by Harley et al. [3] focused on the integration of ethical hacking in preparing future cybersecurity professionals. It underscored the growing sophistication of cyberthreats and the necessity of providing students with the tools and techniques to counteract these threats effectively. Simulation-based platforms were identified as an essential component for bridging the gap between classroom learning and real-world application.

A hands-on approach was further explored by Hu [4], who introduced the concept of leveraging advanced persistent threat (APT) scenarios through ethical hacking labs. The study demonstrated how such labs enable students to simulate real-world attack scenarios, enhancing their problem-solving abilities and practical skills. Similarly, Young et al. [5] highlighted the value of applied courses in ethical hacking, where students actively engage with security assessment tasks for real-world clients. This approach not only enriches technical competencies but also fosters collaboration and professionalism.

The role of sustainable and accessible tools was explored by Dorin [6], who advocated for eco-friendly, portable platforms in ethical hacking education. The study demonstrated how repurposed hardware and modular systems could reduce costs and improve accessibility, particularly in resource-constrained institutions. Moreover, the development of virtual laboratory environments, as discussed by other studies Alfa [7], provided evidence for their efficacy in training students in penetration testing without the need for expensive physical infrastructure.

In alignment with these findings, the PentestHUB platform builds on the OWASP Top 10, OWASP ASVS, OWASP Automated Threat Handbook, OWASP API Security Top 10, and OWASP Top 10 Privacy Risks, MITRE Common Weakness Enumeration, The Web Application Security Consortium list of threats and vulnerabilities to provide a robust learning environment focused on web application security. As noted in previous literature, aligning educational objectives with current industry standards, such as OWASP, MITRE, WASC ensures students gain relevant, job-ready skills. This platform fills a critical gap by providing simulation-based challenges that foster a structured development of ethical hacking skills while reinforcing theoretical knowledge through practical application.

3. Methodology

The development of the PentestHUB platform followed a structured approach that included several key stages. At the initial stage, an analysis of existing ethical hacking training platforms was conducted. The next step was to research market needs and industry standards, including OWASP Top 10, OWASP ASVS, and OWASP API Security Top 10, etc. This allowed us to define learning objectives and develop a conceptual model of the platform that would meet modern cybersecurity and training requirements.

Next, the platform was designed, which included the development of necessary functionality. A technology stack was chosen to ensure the platform's efficiency, scalability, and flexibility. Special

attention was paid to dynamic task checking, automatic saving of user progress, and interactive interaction.

The development included the creation of both client and server sides, integration of key features such as automatic task checking, real-time feedback, and structured training modules. The platform's code was designed to be easily expandable, allowing new challenges and scenarios to be added in response to changing threats in cyberspace.

The next step it was to develop challenges of varying levels of complexity and categories. The tasks were aimed at modeling real-world threats, ranging from simple training cases to complex multi-level attacks. The modular structure ensured the gradual development of students' skills.

The overall methodology is shown below on figure 1.

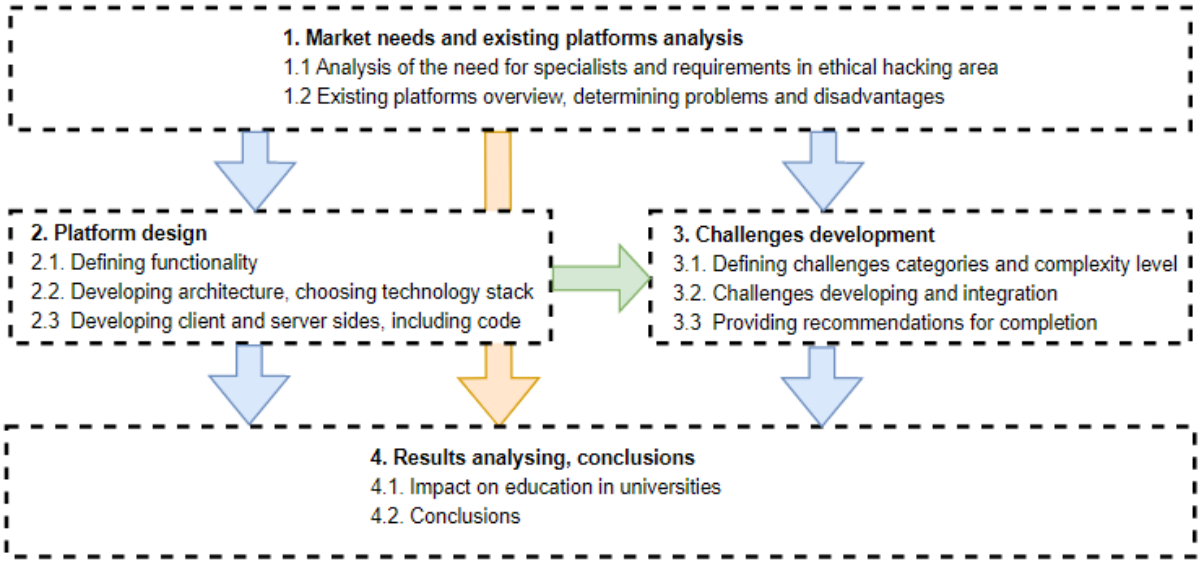

Figure 1: Methodology.

4. Market needs and existing platforms analysis

4.1. Market analysis

The demand for ethical hacking and pentesting specialists has increased significantly in recent years due to the growing number of cyberattacks and the digitalization of business. According to the ISC2 study, the global shortage of cybersecurity professionals in 2024 reached 4.8 million jobs, which is 19% more than in the previous year. This indicates an acute shortage of qualified personnel and, accordingly, high career prospects for experts in this field [8].

The Ukrainian cybersecurity market is also showing rapid growth. Over the past eight years, it has quadrupled to $138 million in 2024, and is expected to grow by another 50% in the next five years [9]. At the same time, the number of cyberattacks is also increasing: in 2023, 2544 cyber incidents were recorded in Ukraine, which is 16% more than in 2022. This poses a serious challenge for businesses and government agencies that need highly qualified specialists to protect digital assets [10].

The demand for cybersecurity professionals directly drives the need for specialized training programs in ethical hacking and pentesting. For such professionals, skills in programming languages (Python, JavaScript), knowledge of Linux and Windows operating systems, understanding of network protocols (HTTP, TCP, DNS), and experience in using basic pentesting tools such as sqlmap, Burp Suite, Nmap, Metasploit, Wireshark are important [11]. Knowledge of penetration testing methodologies, such as OWASP Top Ten, OWASP ASVS, etc. is also important, and having OSCP, OSWE, CEH certificates is a significant advantage during employment.

Although universities can train cybersecurity professionals, traditional curricula often focus on theoretical knowledge, which creates a lack of practical experience among graduates. Working in the field of ethical hacking requires real-world skills in security testing, attack modeling, and the use of specialized tools, which are often not taught in university programs or are only superficially taught. This forces students and young professionals to look for additional learning opportunities outside of universities.

Many future ethical hackers learn through online courses, both paid and free. Paid programs, such as Offensive Security or EC-Council certification courses, provide a deep dive into security testing and provide industry-recognized certifications. At the same time, popular free resources such as HackTheBox, TryHackMe, or CTF platforms allow you to gain practical skills in a gamified learning format. Self-education is becoming a key path for many students, as it provides access to real-life cases and practical tasks that are lacking in traditional curricula [11].

Thus, the cybersecurity market, both in Ukraine and globally, is experiencing rapid growth, and the need for ethical hackers and penetration testers continues to grow. At the same time, the problem of insufficient practical training of university graduates is forcing future professionals to look for alternative learning methods. This creates an important niche for the development of modern educational initiatives that combine academic training with practical cases and interactive learning.

4.2. Existing platforms analysis

There are a number of platforms designed to teach ethical hacking and penetration testing. They have different approaches to training: from lab environments with intentionally vulnerable web applications to interactive gamified solutions. However, each of them has both advantages and limitations. To create an effective learning platform, it is important to evaluate existing solution. Below is a detailed analysis of four popular platforms, such as DVWA [12], Badstore [13], Hackxor [14] and HackThisSite [15].

DVWA is a PHP web application that runs on a MySQL database server. It is specially designed to be vulnerable, giving users the opportunity to practice various attacks such as XSS, CSRF, SQL injection, file injection, and others. DVWA offers three levels of security: low, medium, and high, allowing users to gradually increase the complexity of tasks. The application also provides access to the source code, which helps to understand the inner workings of vulnerabilities.

Badstore simulates an online store and is one of the most vulnerable web applications to practice with. It contains vulnerabilities such as XSS, SQL injection, clickjacking, and weak password hashing (MD5). Users can explore the robots.txt file for further exploits. To use Badstore, you need to download a virtual machine and run it on VMware Workstation. Once configured, the application can be accessed through a browser using the virtual machine's IP address.

Hackxor is a web-based game designed to practice hacking skills. It offers realistic attack scenarios including XSS, CSRF, and SQL injection. There is an online version with two levels and a downloadable version with more advanced levels. The game is aimed at advanced users who want to improve their skills in a realistic environment.

HackThisSite is an online community that provides free computer security learning resources. It offers a variety of tasks that simulate real-world scenarios, including realistic missions, additional tasks, forensic tasks, and programming missions. Each task has its own discussion forum, allowing users to interact and share knowledge [16, 17].

For the comparison the next criteria were chosen. First of all, it is important to compare these solutions for covering different types of risks or vulnerabilities from known lists or documents such as the OWASP Top 10, OWASP ASVS, OWASP Automated Threat Handbook, OWASP API Security Top 10, and OWASP Top 10 Privacy Risks, MITRE Common Weakness Enumeration, The Web Application Security Consortium. Next criteria related to platforms functionality and ability for customization.

Below is a comparison table of these four platforms by key criteria (see table 1). The following assessment levels were selected: 0 - N/A (Not Applicable), 1 – very poor, 2 – poor, 3 – medium, 4 – good, 5 – excellent.

The evaluation was divided into objective and subjective categories. Coverage of OWASP Top 10,

Table 1
Comparison of web security training platforms.

Criteria	DVWA	Badstore	Hackxor	HackThisSite
OWASP TOP 10	Medium	Medium	Medium	Medium
OWASP ASVS	N/A	N/A	N/A	N/A
OWASP Automated Threat Handbook	N/A	N/A	N/A	N/A
OWASP API Security Top 10	N/A	N/A	Very poor	N/A
OWASP Top 10 Privacy Risks	N/A	N/A	N/A	Very poor
MITRE Common Weakness Enumeration	Medium	Medium	Medium	Medium
The Web Application Security Consortium	N/A	N/A	N/A	N/A
Gamification (missions, levels, competitions)	N/A	N/A	Good	Good
Automatically verify solutions	N/A	N/A	N/A	N/A
Possibility to add your own scenarios	N/A	N/A	N/A	N/A
Interactive tips and training	N/A	N/A	N/A	N/A
Integration with tools (Burp Suite, sqlmap, Ghidra)	Good	Poor	Medium	Medium

OWASP ASVS, OWASP Automated Threat Handbook, OWASP API Security Top 10, OWASP Top 10 Privacy Risks, MITRE CWE, WASC and integration with specialized tools were verified through direct analysis of each platform's documentation and functional capabilities. In contrast, gamification effectiveness, the quality of interactive tips, and overall user experience were assessed by a panel of cybersecurity instructors and practitioners who tested each platform and reached consensus on these subjective aspects.

An analysis of existing training platforms for penetration testing (DVWA, Badstore, Hackxor, HackThisSite) showed that they have significant limitations and do not cover modern cybersecurity risks.

Most platforms have not been updated for a long time and do not support the ability to add new vulnerabilities or create custom scenarios. This leads to the fact that they quickly become outdated and do not meet the current realities of cybersecurity.

None of the platforms takes into account the modern OWASP API Security Top 10, OWASP ASVS, OWASP Privacy Risks, as well as MITRE CWE and The Web Application Security Consortium (WASC). This creates an information gap between theoretical standards and practical cybersecurity skills.

Users have to check their attacks on their own without any feedback or automatic analysis. The lack of interactive hints or an explanation system makes learning less effective for beginners. Moreover, it is impossible to customize mentioned platforms that can be an issue for HEIs, to meet modern requirements.

Based on the identified shortcomings, it is clear that it is necessary to develop a modern, flexible, and scalable platform for penetration testing (ethical hacking) training.

5. Platform design

This section describes concept, overall architecture, technologies that were used for developing our platform for enhancing ethical hacking skills, in particular how to identify and exploit vulnerabilities from well-known lists, such as OWASP Top 10, OWASP ASVS, OWASP API Security Top 10, etc. The offer platform is basically a vulnerable web application, in our case it is a webstore.

5.1. Concept and original contribution

PentestHUB was conceived and developed by the authors to address key limitations in existing penetration testing training platforms. While solutions such as DVWA, Badstore, and Hackxor provide basic security challenges, they often lack regular updates, coverage of modern security standards (e.g., OWASP ASVS, OWASP API Security Top 10), and extensibility for creating new scenarios. These shortcomings make them less effective for structured and up-to-date cybersecurity education.

The idea behind PentestHUB was to create an interactive, simulation-based platform that bridges the gap between theory and practice. Our approach integrates real-world security vulnerabilities aligned with established standards, enabling learners not only to exploit security flaws but also to analyze the corresponding source code and understand remediation techniques. Additionally, PentestHUB offers a dynamic and scalable environment where new challenges can be added as cybersecurity threats evolve. This makes it suitable for academic institutions and professional training programs aiming to provide a comprehensive hands-on experience in ethical hacking.

5.2. Architecture and technologies

The PentestHUB is implemented in JS (Java Script) and TS (Type Script) programming languages. For frontend, we used one of the popular frameworks Angular, it is also called as single page application. The Google Material Design with Angular Material components were used for creating GUI (graphical user interface). The Angular Flex-Layout was used to achieve appropriate responsiveness.

Backend of the platform was implemented with the JS and the TS. An Express application deployed on a Node.js server sends to the browser the client-side code. For the appropriate backend functionality to the client, the RESTful API was used. As the underlying DB (database), we used SQLite for its file-based nature. This makes the DB easy to create from scratch programmatically without the need for a dedicated server. It was also necessary to create an abstraction layer from DB. For this purpose, we used the Sequelize and finale-rest. These tools provide ability to use dynamically created API endpoints for simple interactions with DB resources while also allowing for the execution of custom SQL for more complex queries.

PentestHUB also has an additional DB, the MarsDB. It is a JS implementation of the popular MongoDB NoSQL database that is compatible with almost all of its query/modify procedures.

The WebSocket Protocol was used to provide push notifications after challenge is successfully done. We also implemented user registration in the simplest way with OAuth 2.0. It allows every user to sign in with Google accounts.

The architecture, communication between client, server and data layers are shown on figure below (see figure 2).

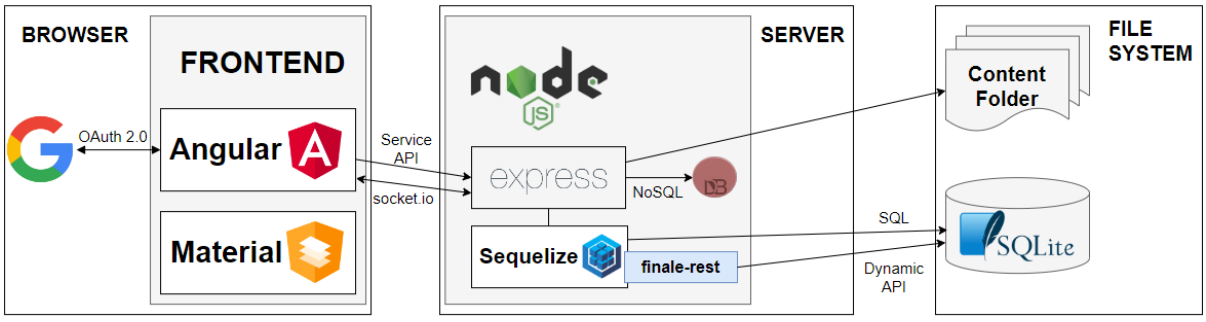

Figure 2: The PentestHUB architecture and communication layers.

5.3. Platform overview

To launch developed platform, the Node JS command prompt should be installed. Then, it is necessary just simply switch to the platform directory and run “npm start” command (see figure 3). After that platform will be available in the browser with the URL localhost:3000.

First of all, user will see welcome banner (figure 4) and then it will be possible to take a look on webstore with different tools, software, etc. for ethical hacking.

We integrated a score board with available challenges. Each task has its own level and is associated with a certain vulnerability. Also, each challenge has its own tag or a few tags:

- **Shenanigans** indicates a task that is not considered serious and/or realistic, but is more for fun.

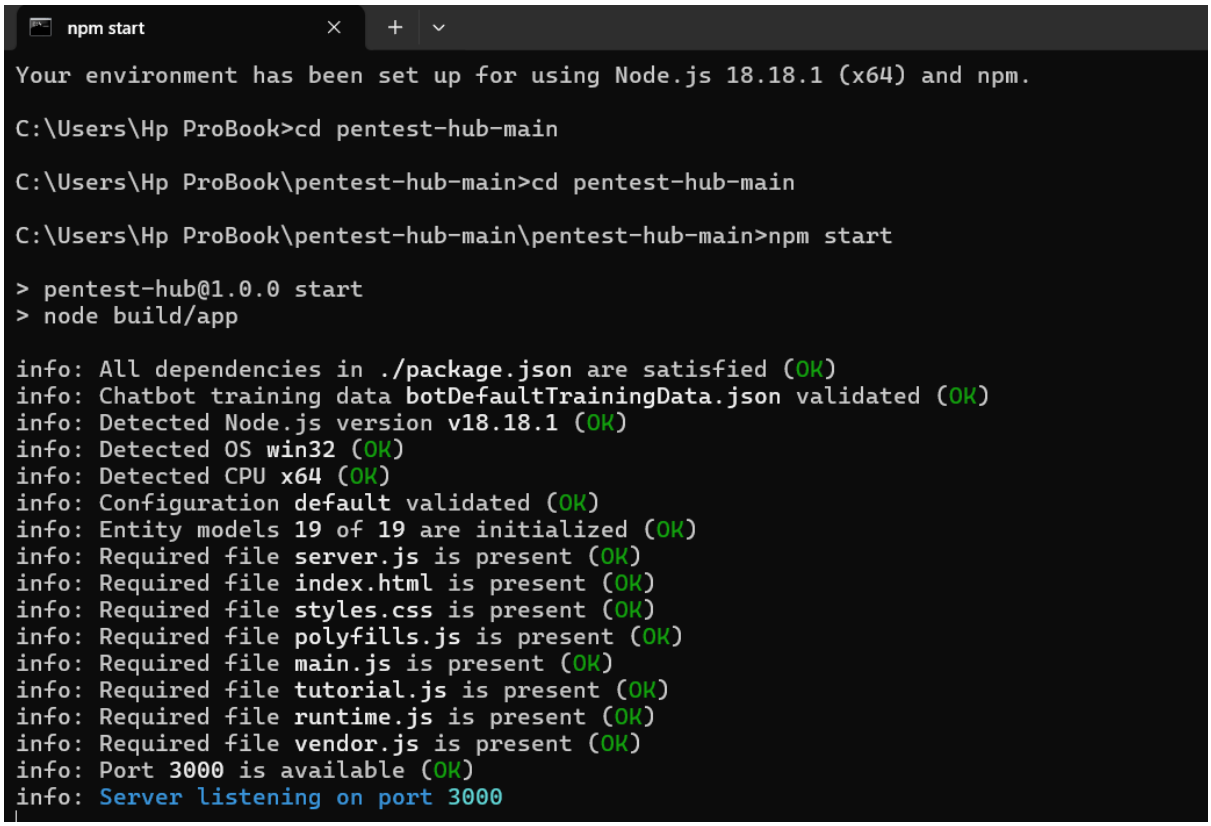

Figure 3: Platform launching.

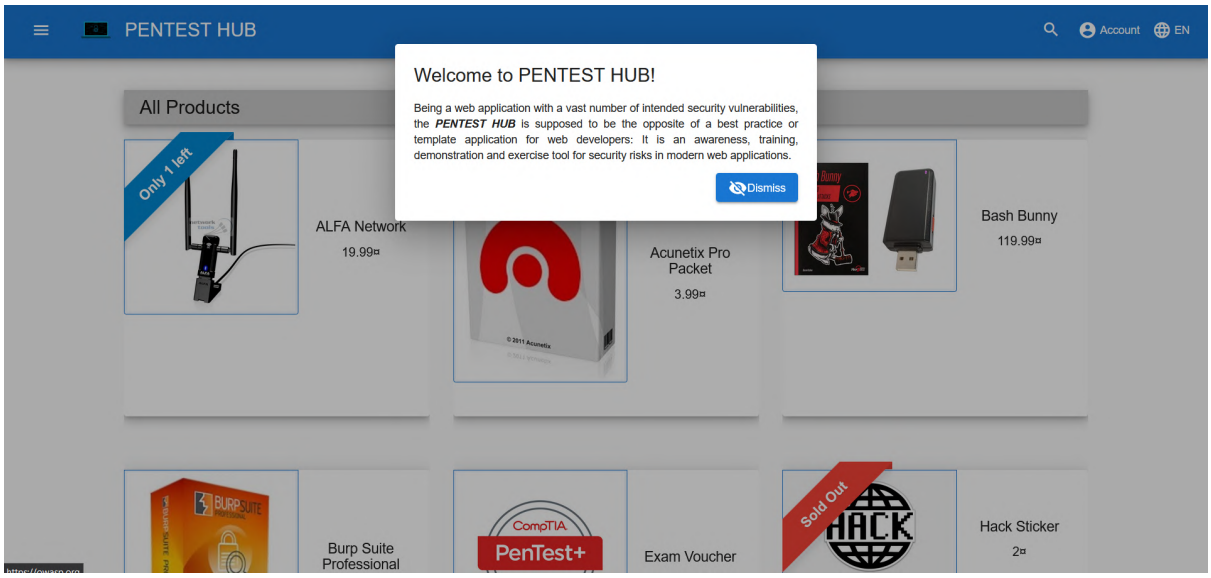

Figure 4: Launched platform.

- **OSINT** indicates tasks that require some online research or social surveillance outside of the program.
- **Good Practice** highlights issues that are not so much about vulnerabilities as they are about promoting good practices (security).
- **Danger Zone** indicates potentially dangerous tasks that are disabled by default on Docker/Heroku due to RCE (Remote Code Execution) or other risks.
- **Good for Demos** highlights tasks that are suitable for live demonstrations or awareness training.

- **Prerequisite** highlights tasks that must be completed before one or more other tasks can be completed.
- **Brute Force** indicates a task where the use of an automation tool or custom script is an option or even a prerequisite.
- **Tutorial** indicates tasks where there is a hacking instructor script to help beginners.
- **Code Analysis** indicates tasks where it may be useful to dig into the source code of the program.

The user's progress is automatically saved. It is possible to back up and restore the progress. There is also a self-healing function of the PentestHUB platform - deleting the progress from the database when the server starts.

This page is shown on figure 5.

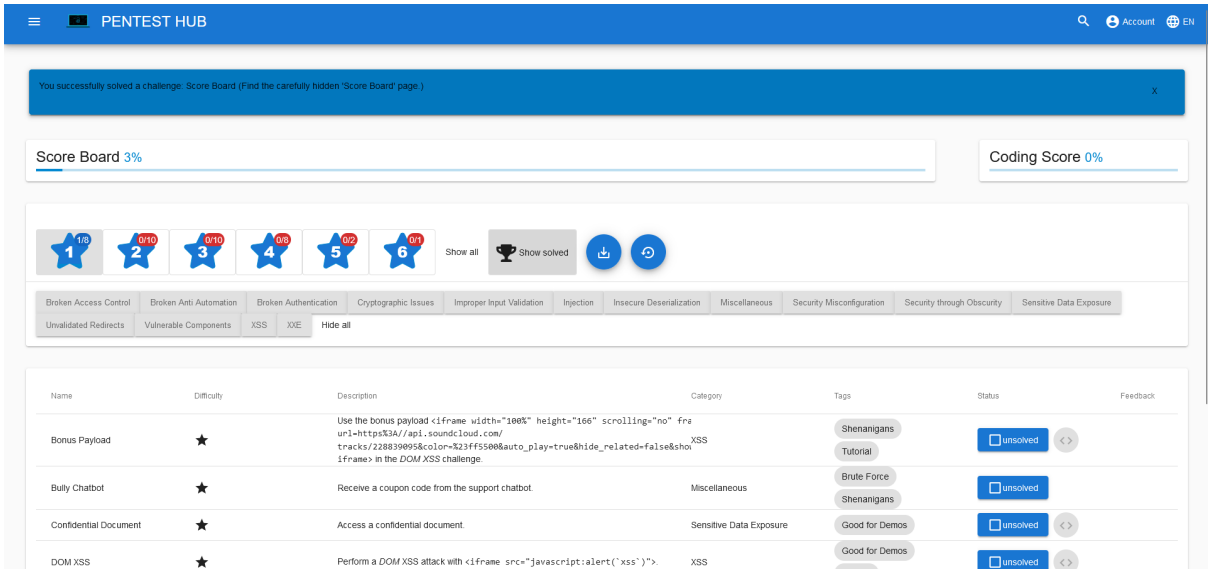

Figure 5: The Score Board page.

6. Developed challenges

As was mentioned before, we associate each challenge with typical web application vulnerabilities. The following diagram shows number of challenges by each category (figure 6). Total number of challenges is 39.

As a special feature is that for many tasks, we have also implemented the "Code Issues" task (figure 7). An additional button is available that opens a dialog box containing the actual code snippet responsible for the security vulnerability underlying a particular task. This snippet is downloaded in real time from the actual codebase of the running application and is cleaned up to not show "task checking" or similar code that would not be present in a real application. User can try to identify the actual lines of code responsible for the vulnerability behind a particular issue. After submitting user's choice, the server will provide feedback on the choice. If the correct lines are submitted, user will be offered 3-4 possible options for fixing the vulnerability. User can use the built-in code comparison to review them and then select what user think is the correct fix. Sending user's choice to the server will result in feedback again.

6.1. Challenges overview

There are 15 main categories of integrated challenges. This subsection provides brief description of challenges by each category.

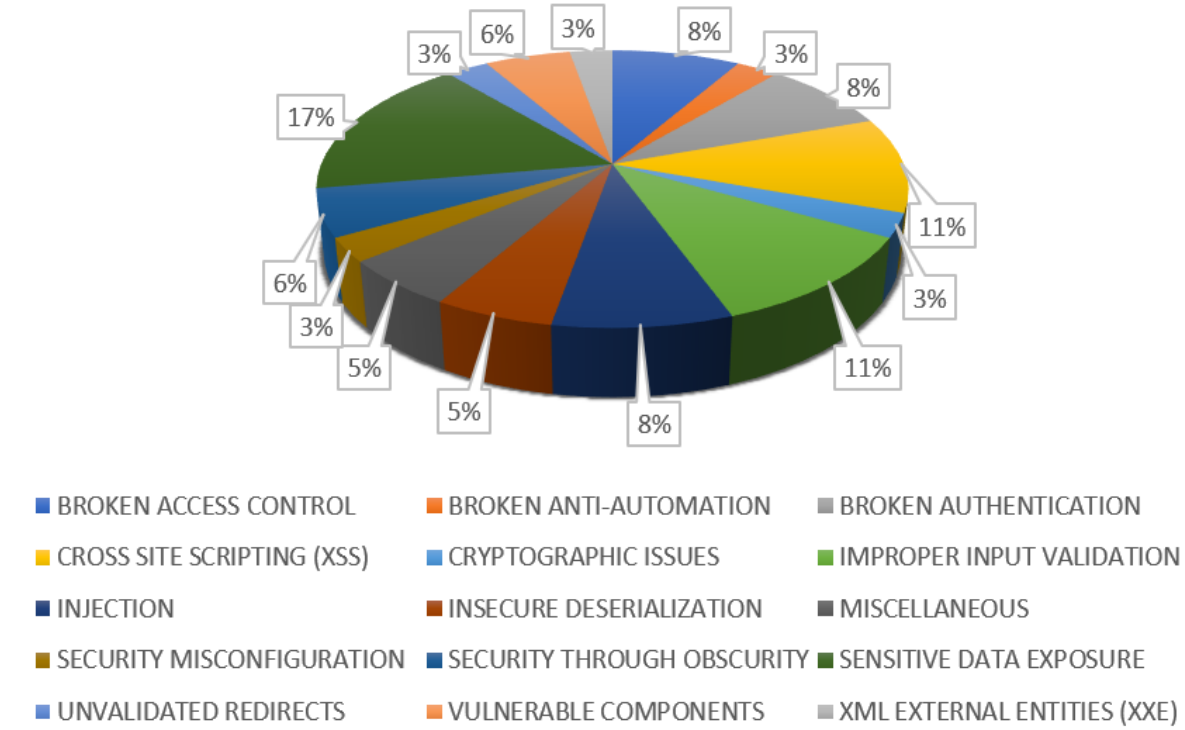

Figure 6: Challenges' categories.

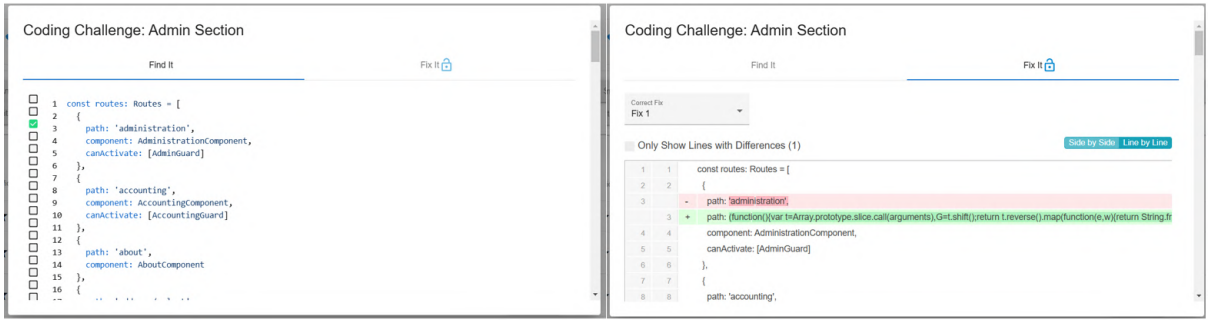

Figure 7: Coding challenge.

1. Broken Access Control. Broken Access Control is a critical vulnerability in web applications that allows attackers to gain unauthorized access to functionality or data. Tasks in this category focus on identifying access configuration errors. For example, the "Admin Section" task requires the identification of the administrative panel, and the "View Basket" task allows the user to access another client's basket by changing the request parameters.
2. Broken Anti-Automation This category covers mechanisms that are supposed to prevent automated attacks. For example, the "CAPTCHA Bypass" task examines the effectiveness of the CAPTCHA mechanism. Students may try to bypass this mechanism by manipulating client or server requests.
3. Broken Authentication Broken Authentication allows attackers to bypass authentication mechanisms. In the "Password Strength" task, students test the strength of administrator passwords, and "Bjoern's Favorite Pet" demonstrates attacks on password recovery mechanisms through social engineering.
4. Cross-Site Scripting (XSS). XSS attacks exploit insufficient validation of input in web applications. "DOM XSS" teaches students how to identify and exploit DOM-based XSS, and "Reflected XSS"

explores the possibilities of reflected scripting attacks.

5. Cryptographic Issues. This category focuses on issues related to the misuse of cryptographic mechanisms. For example, "Weird Crypto" requires analyzing and identifying weak cryptographic algorithms or their misuse.
6. Improper Input Validation. Improper input validation can lead to vulnerability exploitation. "Repetitive Registration" demonstrates the problem of insufficient validation of registration data, and "Expired Coupon" tests the possibility of using expired promotional codes.
7. Injection. Injection attacks allow to execute unwanted commands in internal systems. The "Login Admin" task explores SQL injection to gain administrative access, and the "Database Schema" task involves extracting the database schema by injecting SQL queries.
8. Insecure Deserialization. Insecure deserialization allows to execute arbitrary code on the server. "Blocked RCE DoS" demonstrates how using incorrect deserialization formats can cause a denial of service (DoS), and "Successful RCE DoS" explores how deserialization can be used to execute remote code.
9. Miscellaneous. This category covers a variety of tasks that are not included in other categories but are of significant practical interest. For example, the "Bully Chatbot" task explores the interaction with automated chatbots and how to obtain hidden information from them.
10. Security Misconfiguration. Incorrect security settings can create potential threats. The "Deprecated Interface" task demonstrates the risks of using outdated administration interfaces without proper access restrictions.
11. Security Through Obscurity. This category demonstrates that hiding information is not an effective security strategy. In "Privacy Policy Inspection", students analyze privacy policies to find hidden information, and "Steganography" explores methods of hiding data.
12. Sensitive Data Exposure. This category focuses on the leakage of sensitive information. "Confidential Document" tests document protection mechanisms, and the "GDPR Data Theft" analyzes the possibility of personal data leakage in accordance with GDPR requirements.
13. Unvalidated Redirects. Unvalidated redirects can be used in phishing attacks. "Outdated Allowlist" explores methods of bypassing the restrictions of the list of allowed URLs.
14. Vulnerable Components. Vulnerable libraries and dependencies can pose potential threats. "Vulnerable Library" demonstrates the risks of using outdated dependencies, and "Unsigned JWT" analyzes the possibilities of attacking unsecured JSON Web Tokens (JWTs).
15. XML External Entities (XXE). XXE attacks exploit weak XML parsers. "XXE Data Access" demonstrates the ability to access local files via XML parsing vulnerabilities.

Tools and gained practice skills. To perform tasks on the PentestHUB platform, knowledge how to use different tools for ethical hacking can be gained, such as Burp Suite, DevTools of different browsers, Postman, sqlmap, Hydra, OWASP ZAP and others. Each of them helps to analyze and exploit different types of vulnerabilities.

During these tasks, students learn how to find and exploit vulnerabilities, bypass security mechanisms, use Open-Source Intelligence (OSINT) to gather information, test authentication and verify input data, perform SQL and XSS injections, analyze cryptographic mechanisms, and work with deserialization. These skills are critical for ethical hackers and cybersecurity professionals.

6.2. Recommendations for completion

We recommend browsers for completing tasks such as Chrome or Mozilla Firefox. They have powerful developer tools called DevTools. To intercept proxies, we recommend to use BurpSuite or OWASP ZAP.

When performing tasks related to SQL Injection, users can use sqlmap to learn how to work with this tool. Mozilla Firefox has built-in capabilities for forging HTTP requests, and for Google Chrome, users will need to download the Tamper Chrome extension. An API testing plugin such as PostMan for Chrome allows users to interact with the RESTful backend of a web application directly. Skipping the interface can often be useful for bypassing client-side security mechanisms or simply to complete

certain tasks faster. Here, users can create requests for all available HTTP verbs (GET, POST, PUT, DELETE, etc.) with different content types, request headers, etc. If users feel more comfortable with the command line, curl will work just as well as the recommended browser plugins. Note that instead of downloading all the plugins and tools to users' computer, users can use a virtual machine with the Kali Linux distribution, which already has a large number of useful and powerful tools for penetration testing. However, all tasks can only be performed using a browser.

7. Impact on education in universities

HEIs education in the field of cybersecurity is facing significant challenges due to the rapid development of digital technologies and the growing number of cyber threats and its complexity. Despite the existence of academic programs that cover theoretical aspects of security, a significant part of the courses remains disconnected from the practical component. This is due to limited access to real penetration testing cases, lack of dynamically updated learning platforms, and insufficient integration of modern cybersecurity standards, such as OWASP Top 10, OWASP API Security Top 10, OWASP ASVS, and MITRE CWE, into the educational process.

Traditional teaching methods often focus on the study of concepts, regulations, and analysis of general attack principles, but they do not provide students with the opportunity to test their knowledge in a practical environment. This leads to a situation where graduates, while having theoretical training, do not have the necessary skills to work with real systems and tools. Research shows that effective cybersecurity training should be based on active learning methods, including laboratory classes, interactive attack simulations, and pentesting scenarios in controlled environments.

The developed PentestHUB training platform is designed to address these issues by providing students with a dynamic, practice-oriented environment for researching information system, in particular web application, vulnerabilities. Thanks to the integration of multi-level attack scenarios, the platform will allow creating training programs adapted to different levels of students' training, from beginner to expert. In particular, the ability to customize the complexity of tasks will facilitate gradual immersion in the penetration testing process, which is in line with modern pedagogical approaches to teaching technical disciplines.

Also, university courses are often limited to a theoretical discussion of attacks, which does not give students the opportunity to analyze and fix vulnerabilities directly in the program code. The developed learning platform eliminates this drawback by integrating code analysis tasks. For many practical tasks, additional functionality is available on the scoreboard, which opens a source code snippet containing the corresponding vulnerability. This allows students not only to test attacks but also to identify vulnerable lines of code, which is a critical skill for future cybersecurity professionals.

It is also worth noting that the integration of such platforms into the educational process of universities helps to improve the methodology of teaching cybersecurity. Educators receive a tool to create customized laboratory tasks that meet the requirements of specific curricula and can conduct real-time assessment monitoring of student performance.

7.1. Case study

Within the "Veterano IT Cluster" project ledded by the Scientific Cyber Security Association of Ukraine, several military veterans underwent specialized cybersecurity training before beginning internships at LLC "Smart Power", focusing on web application penetration testing. As part of their on-the-job learning, the PentestHUB platform was introduced to help them rapidly apply theoretical concepts in a controlled environment.

Over a four-week period, interns engaged with curated PentestHUB challenges that spanned all used common vulnerabilities lists in developed platform. They practiced both offensive and defensive techniques, leveraging the platform's real-time feedback and code-analysis feature to refine their exploit methods and improve remediation strategies. Mentors observed that participants quickly moved from basic "trial-and-error" hacking attempts to more structured, analytical approaches, an evolution reflected

in their challenge completion rates and reduced error counts. Several interns highlighted the value of immediate, automated hints, noting that this format provided a tangible sense of progress and confidence as they tackled successively harder tasks.

An informal survey of participants revealed that most considered PentestHUB an integral part of their learning process, emphasizing the platform's hands-on nature and practical alignment with real-world penetration testing procedures. According to the supervising mentors, the structured progression of exercises helped interns grasp essential security concepts faster compared to conventional lecture-style training. By the end of the internship, interns consistently demonstrated greater proficiency in recognizing, exploiting, and mitigating application-level vulnerabilities. This case study thus illustrates how PentestHUB accelerates practical skill acquisition, particularly for individuals transitioning into the cybersecurity field, and underscores the platform's potential for broader adoption in professional development.

7.2. Proposed pilot implementation plan in HEI

We propose a concise pilot study to integrate PentestHUB into a "Web Application Security" course at Kyiv Aviation Institute, spanning four weeks and involving approximately 20 advanced students. Half will form a control group using traditional lab materials, while the other half (the experimental group) will supplement the same labs and PentestHUB challenges, focusing on OWASP Top 10 vulnerabilities. Both cohorts will complete a pre-test to gauge baseline knowledge, then undergo parallel practice sessions. The experimental group will benefit from PentestHUB's real-time feedback and code-analysis features, whereas the control group will rely on standard exercises and instructor guidance.

At the end of the four weeks, all participants will take a common post-test featuring a practical scenario with hidden vulnerabilities and short theoretical questions. Their performance will be compared to assess how PentestHUB influences vulnerability detection and remediation skills, as well as overall conceptual understanding. Brief surveys and informal interviews will gather additional insights on usability and perceived learning gains. This pilot plan aims to validate PentestHUB's educational impact and establish a framework for broader course integration and iterative improvements.

8. Conclusions

The development of ethical hacking skills is a key component of modern cybersecurity education. Traditional educational approaches, which focus mainly on theoretical aspects, do not provide a sufficient level of practical training to effectively counter modern cyber threats. The introduction of interactive platforms, such as the PentestHUB, allows for the creation of a balanced learning environment that combines theory with practice.

The developed PentestHUB platform is aimed at bridging the gap between academic education and the real requirements of the industry. It offers an interactive environment for simulating attacks and exploring web application vulnerabilities based on modern security standards such as OWASP Top 10, OWASP ASVS, OWASP API Security Top 10, MITRE CWE, etc. It also provides an opportunity for gradual learning by categorizing tasks by difficulty level, automatically saving progress, and integrating with popular security testing tools.

An analysis of existing pentesting (ethical hacking) training platforms has shown that most of them have significant limitations, such as the lack of scenario expansion, outdatedness, or lack of interactivity. The PentestHUB stands out among them with its flexibility, modern approach to training, and focus on the practical skills needed to work in the cybersecurity field.

Integration of the PentestHUB into HEIs curricula improves the quality of training, providing them with the ability to not only identify but also fix vulnerabilities in real code. The use of such platforms in the educational process contributes to the development of critical thinking, deepening knowledge of cybersecurity and increasing the competitiveness of graduates in the labor market.

Thus, the PentestHUB is an important step in improving cybersecurity education and forming a new generation of professionals capable of effectively responding to modern digital security challenges.

Author Contributions

Conceptualization, Alla D. Pinchuk and Oleh O. Polihenko; methodology, Roman S. Odarchenko; software, Alla D. Pinchuk and Oleh O. Polihenko; writing – original draft, Alla D. Pinchuk and Roman S. Odarchenko; writing—review and editing, Roman S. Odarchenko. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Data Availability Statement

No new data were created or analysed during this study. Data sharing is not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work was supported by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060) and "Methods of building protected multilayer cellular networks 5G/6G based on the use of artificial intelligence algorithms for monitoring country's critical infrastructure objects" (# 0124U000197).

Declaration on Generative AI

During the preparation of this work, the authors used X-GPT-4 in order to assist with writer's block, translate text from Ukrainian into English, and correct grammatical errors, typos.

References

[1] C. Li, Penetration testing curriculum development in practice, Journal of Information Technology Education: Innovations in Practice 14 (2015) 85–89. doi:10.28945/2189.

[2] R. Hartley, Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack, Journal of International Technology and Information Management 24 (2015) 95–104. doi:10.58729/1941-6679.1055.

[3] R. Harley, D. Medlin, Z. Houlik, Ethical hacking: Educating future cybersecurity professionals, in: Proceedings of the EDSIG Conference, Appalachian State University, 2017. URL: https://www.researchgate.net/publication/320474715_Ethical_Hacking_Educating_Future_Cybersecurity_Professionals.

[4] Y.-H. Hu, Providing A Hands-on Advanced Persistent Threat Learning Experience Through Ethical Hacking Labs, Journal of The Colloquium for Information Systems Security Education 9 (2022). doi:10.53735/cisse.v9i1.153.

[5] J. Young, K. Campbell, A. Fanti, S. Johnson, Z. Sells, A. Sutter, The development of an applied ethical hacking and security assessment course, in: Proceedings of the Twelfth Midwest Association for Information Systems Conference, Bradley University Center for Cybersecurity, Springfield, Illinos, 2017. URL: https://www.researchgate.net/publication/334455131_The_Development_of_an_Applied_Ethical_Hacking_and_Security_Assessment_Course.

[6] M. Dorin, The eco-friendly hacker: Asustainable lab for teachingethical hacking, South Sustainability 5 (2024). doi:10.21142/SS-0501-2024-e100.
[7] F. A. Alfa, Design and implementation of web application for cybersecurity education enhancement: Developing specialized software for practical skill development in penetration testing. (2024). doi:10.13140/RG.2.2.13722.56000.
[8] A. Rybenko, Demand for cybersecurity specialists is growing worldwide: experts explain why, 2025. URL: https://happymonday.ua/fakhivtsi-z-kiberbezpeky-staiut-bilsh-zatrebuvanymy.
[9] E. B. Association, Ukrainian cybersecurity market has quadrupled in eight years, 2025. URL: https://eba.com.ua/ukrayinskyj-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/.
[10] A. Sergienko, Cybersecurity market in Ukraine: growth, challenges and innovations, 2025. URL: https://speka.media/rinok-kiberbezpeki-v-ukrayini-rist-vikliki-ta-innovaciyi-93lyx4.
[11] 10Guards, Pentester: the profession of an ethical hacker, 2022. URL: https://10guards.com/ua/blog/2022/02/21/pentester-the-profession-of-ethical-hacker/.
[12] GitHub, GitHub - digininja/DVWA: Damn Vulnerable Web Application (DVWA), 2015. URL: https://github.com/digininja/DVWA.
[13] VulnHub, Badstore: 1.2.3, 2025. URL: https://www.vulnhub.com/entry/badstore-123,41/.
[14] Hackxor, Hackxor , 2012. URL: https://hackxor.net/.
[15] HackThisSite, HackThisSite, 2016. URL: https://www.hackthissite.org/.
[16] S. Vashist, Top 5 (deliberately) vulnerable web applications to practice your skills on, 2018. URL: https://www.infosecinstitute.com/resources/penetration-testing/top-5-deliberately-vulnerable-web-applications-to-practice-your-skills-on/.
[17] GeneAka, 25+ Vulnerable websites to practice your ethical hacking skills, 2022. URL: https://genesis-aka.net/information-technology/professional/2022/05/11/25-vulnerable-websites-to-practice-your-ethical-hacking-skills/.