# Sifu Reloaded: An Open-Source Gamified Web-Based CyberSecurity Awareness Platform

**José Carlos Paiva**
CRACS – INESC TEC, Porto, Portugal
DCC – FCUP, Porto, Portugal

**Ricardo Queirós**
CRACS – INESC TEC, Porto, Portugal
uniMAD – ESMAD, Polytechnic of Porto, Portugal

**Tiago Gasiba**
Siemens AG, München, Germany
Universität der Bundeswehr München, Germany

## Abstract

Malicious actors can cause severe damage by exploiting software vulnerabilities. In industrial settings, where critical infrastructures rely on software, handling these vulnerabilities with utmost care is crucial to prevent catastrophic consequences. For this purpose, a cybersecurity awareness platform called Sifu was created. This platform automatically assesses challenges to verify its compliance to secure coding guidelines. Using an artificial intelligence method, an interactive component provides players with solution-guiding hints. This paper presents an improved version of the Sifu platform, which evolves the tool in the following aspects: architecture, data model and user interface. The new platform separates the server and client-side using a REST API architecture. It also accommodates an intrinsic and richer layer of gamification, which explores the concept of game rooms at an organizational and gamification level. Finally, it offers an improved interactive training experience for individuals and organizations through a responsive and intuitive single-page web application.

**2012 ACM Subject Classification** Applied computing → Interactive learning environments; Applied computing → E-learning; Applied computing → Computer-managed instruction; Applied computing → Computer-assisted instruction; Security and privacy

**Keywords and phrases** learning environment, cybersecurity, challenges, gamification, automatic assessment

**Digital Object Identifier** 10.4230/OASIcs.ICPEC.2023.5

**Category** Short Paper

**Funding** This work is financed by National Funds through the Portuguese funding agency, FCT – Fundação para a Ciência e a Tecnologia, within project LA/P/0063/2020.

## 1 Introduction

In an increasingly interconnected world, the importance of cybersecurity awareness cannot be overstated. The rapid proliferation of digital technologies and increased cyber threats demand proactive measures to safeguard critical infrastructures. As malicious actors continue to exploit software vulnerabilities, there is a need for practical and effective cybersecurity awareness training that gives individuals and organizations the knowledge and skills to defend against cyber threats. In [3], the Sifu platform was introduced. This platform aims to increase cybersecurity awareness of software developers on secure coding. The Sifu platform, embedded in cybersecurity challenge (CSC) events, is a successful artifact among industrial software developers. CyberSecurity Challenges is a game that targets software developers and was inspired in the Capture-the-Flag (CTF) type of game. In CTF games, the participants


© José Carlos Paiva, Ricardo Queirós, and Tiago Gasiba;
licensed under Creative Commons License CC-BY 4.0

are presented with challenges related to cybersecurity in a competitive environment. Upon solving the challenges, the players earn points. The player or team with the most points wins the game.

However, the Sifu platform needs a consolidated gamification aspect and cannot easily be used as a stand-alone application (i.e., separated from CSC events). An improved Sifu platform was developed to address these issues, which we call SifuV2. The new platform profits from the authors' long experience with the original Sifu platform, players' feedback on user experience, and the author's experience in designing gamified applications. The newly evolved platform can empower individuals and organizations in the battle against cyber risks.

This paper aims to introduce the new features and capabilities of this web-based cybersecurity awareness platform based on architecture, data model, and user interface. In the architecture facet, this new version separates client and server through an API complying with REST (Representational State Transfer). The importance of REST architectures lies in their ability to provide scalable, interoperable, and flexible systems that can easily integrate with other services. By adhering to REST principles, developers can build robust, distributed, and easily maintainable software systems that meet the demands of modern web and mobile applications. The second facet is the data model, which adds a new layer of gamification, exploring the concept of game rooms both from an organizational perspective and to gamify the environment. Including gamification elements, such as quizzes, challenges, and rewards, enhances user engagement and motivation, transforming cybersecurity education into an enjoyable and immersive experience.

Additionally, the platform was changed to provide an improved user experience through an intuitive user interface. Here, learners can access a rich array of interactive training modules and engaging videos through a responsive single-page web application.

In the subsequent sections of this paper, we will explore related work, in particular, other web-based cybersecurity awareness platforms. In section 3, we present the evolved platform's architecture, and enumerate the data model changes regarding the previous version. Additionally, we introduce the new user interface. In the last section, the contributions of this article to the scientific community are presented, and future work is briefly discussed.

## 2 Related Work

Table 1 and Table 2 depict currently available cybersecurity awareness training platforms. These platforms typically offer a combination of training modules, phishing simulations, knowledge assessments, and reporting capabilities to help organizations educate their employees about cybersecurity threats and promote a culture of security awareness. Among these, we can find the following training platforms:

- **Cybrary**[1]: offers a wide range of cybersecurity courses, which covers various topics such as network security, ethical hacking, and incident response. This platform is offered as a free or as a paid version. The platform includes the option to earn cybersecurity certifications.
- **Hack The Box**[2]: a platform offering a range of realistic virtual machines for penetration testing practice. It provides challenges and labs allowing participants to test their skills in a controlled environment. Access to some machines and features requires a paid subscription, but a free option is also available.

[1] `https://www.cybrary.it`
[2] `https://www.hackthebox.eu`

- **TryHackMe**[3]: is a platform that teaches cybersecurity through interactive and gamified content. It offers various rooms with different themes and difficulty levels. Each room includes practical exercises, challenges, and walkthroughs to help players learn and practice cybersecurity concepts.
- **PentesterLab**[4]: provides online courses and hands-on labs specifically designed for web application security. Their courses cover web penetration testing, network security, and secure coding. They offer a mix of free and paid content, with interactive labs for skill practicing.
- **OverTheWire**[5]: is a platform that offers a series of interactive war games designed to teach and practice cybersecurity skills. Each game focuses on a specific area of cybersecurity, such as e.g. basic Linux command-line skills and cryptography. The challenges' difficulty gradually increase, allowing the player to improve their skills progressively.
- **Root-me**[6]: is a platform that offers a wide range of challenges and labs covering various cybersecurity topics, including web security, network security, reverse engineering, and more. It provides a hands-on approach with practical activities to reinforce players' understanding and skills.
- **CTFtime**[7]: while not a training platform, this website aggregates information about existing Capture The Flag (CTF) competitions that take place worldwide.

Evaluating each platform based on the organization's needs and requirements is essential before deciding which to use. In [4], the authors provide guidelines on selecting CTF games to address industrial software developers. Employing a set of well-defined criteria facilitates the comparison of tools, allowing one to make an informed decision and choose the most suitable web-based platform for specific cybersecurity needs. It also provides a structured approach to assess the strengths and weaknesses of each tool, making it easier to identify the best fit for any specific use case.

Predefined criteria were selected and applied to compare cybersecurity tools effectively. The results are presented in two tables according to their pricing models: Table 1 with those that offer both free and paid models (or exclusively paid) and Table 2 with the free tools.

**Table 1** Comparison of paid cybersecurity tools.

| Criteria | Cybrary | Hack The Box | TryHackMe | PentesterLab |
|---|---|---|---|---|
| Year | 2015 | 2017 | 2018 | 2013 |
| OS/Proprietary | Proprietary | Online Platform | Online Platform | Online Platform |
| User Experience | ✓ | ✓ | ✓ | ✓ |
| Course Catalog | ✓ | ✓ | ✓ | ✓ |
| Course Topics | Various | Ethical Hacking | Ethical Hacking | Penetration Testing |
| Challenge Types | N/A | CTF | CTF | N/A |
| Certification | ✓ | × | × | × |
| Gamification | ✓ | ✓ | ✓ | × |
| Automatic Eval. | × | × | × | × |
| Collaboration | ✓ | × | ✓ | ✓ |

[3] https://tryhackme.com
[4] https://pentesterlab.com
[5] https://overthewire.org
[6] https://www.root-me.org
[7] https://ctftime.org

**Table 2** Comparison of free cybersecurity tools.

| Criteria | OverTheWire | Root-me | CTFtime |
|---|---|---|---|
| Year | 2002 | 2004 | 2008 |
| OS/Proprietary | Online Platform | Online Platform | N/A |
| User Experience | ✓ | ✓ | ✓ |
| Course Catalog | ✓ | ✓ | ✓ |
| Course Topics | Networking/Security | Challenges/CTF | Challenges/CTF |
| Challenge Types | Challenges/CTF | Challenges/CTF | Challenges/CTF |
| Certification | × | × | × |
| Gamification | × | × | × |
| Automatic Eval. | × | × | × |
| Collaboration | × | ✓ | ✓ |

Since currently available tools have different pricing models, ranging from free to paid options, this criteria allows users to choose a platform that fits their budget and financial constraints.

All the covered platforms offer a comprehensive course catalog covering various aspects of cybersecurity. This indicates that there are abundant learning opportunities available across different platforms. The tools also cover various course topics, including ethical hacking, penetration testing, networking/security, and challenges/capture the flag. While there is a large variety in the subjects offered, a quality assessment of these is outside the scope of the present work. We refer the reader to [4] for further discussions.

Cybrary is the only platform that offers certifications upon completion of their courses. This is beneficial for individuals looking to enhance their credentials and showcase their skills in the cybersecurity field.

Regarding gamification, Hack The Box, Cybrary, and TryHackMe incorporate several gamification features which can enhance engagement and motivation. The former offers simulations with avatars and narrative scenarios to throw users into classic cyber hacks. The others include gamification features typically found in PBL (Points/Badges/Leaderboards) gamified applications. In terms of collaboration, Cybrary, TryHackMe, Root-me, and CTFtime have collaborative challenges/missions that require teams to work together to accomplish a common goal. In this realm, most tools also offer social features, such as discussion chats and forums, which allows participants to share ideas and build relationships, enhancing collaboration and promoting a sense of community.

Finally, as indicated by the checkmarks, most tools strive to provide a positive user experience. This suggests that they are designed considering usability and accessibility, making it easier for learners to navigate and engage with the platforms.

## 3 SifuV2

Sifu [3] is an open-source web-based platform for cybersecurity awareness that challenges users to fix the source code of a project containing vulnerabilities. User submissions are automatically accepted if the source code complies with secure coding guidelines, does not have known or additional vulnerabilities, and performs the desired tasks. To this end, the analysis of the proposed solution submitted by a user involves several tools (e.g., SonarQube [9], CodeChecker [2], and various unit testing tools) acting on different phases of the analysis, static and dynamic. An intelligent coach processes the result of such analysis to complement the result presented to the learner with a hint.

SifuV2 keeps both the original automated assessment module and the intelligent coach module, which are the central components of Sifu. However, it reformulates the server and client sides. In particular, it separates both by adopting a REST (Representational State Transfer) API architecture on the server side. The REST API is then connected to the front end by a single-page application (client). The REST API is implemented using Flask [8] and is supported with a PostgreSQL database. The following subsections present the significant changes present in the second version of Sifu, which concentrate on the data model and user interface.

## 3.1 Data Model

Sifu v2 aims to redesign the previous version [3] to accommodate an intrinsic and richer layer of gamification rather than only awarding points for correctly solving a challenge presented in an external leaderboard and giving the platform a more formative direction. To this end, it explores the concept of game rooms from an organizational and gameful perspective. Firstly, rooms represent checkpoints of the learning path a player must complete before proceeding to another. Lastly, rooms display the active players solving the challenges simultaneously, track the best performers using a leaderboard, and reward players on successful completion.

Consequently, the data model has been re-implemented to achieve these goals. The most important model components are the following.

**User** represents both administrators and players. Each player has experience points, levels, badges, medals, and a wallet containing coins. Moreover, they have a public profile containing the username, avatar, level, medals, and badges.

**Room** has a set of generally related challenges to be solved (e.g., the same vulnerability or project). Platform administrators create rooms that can be either of the type: "open", "accessed by invite", or "locked by password/access code". Completing a room gives the player one or more rewards, possibly unlocking another room directly (i.e., providing an access code) or indirectly (i.e., achieving a level of experience that enables access to the room). Each room has an internal leaderboard sorted in descending order by the number of solved challenges and, in case of tie, in ascending order of shortest solving time. Furthermore, players can also create duel rooms by using coins. These rooms are open to a limited amount of players, who should pay an established entry fee and run until one of the participants finalizes all challenges. Such participant collects the sum of coins paid by all participants.

**Challenge** is the educational unit of Sifu. The traditional Sifu challenges are projects that contain one or more vulnerabilities, which ask the player to rewrite the code keeping the same functionality but eliminating existing vulnerabilities and following secure coding guidelines and secure software development best practices. Quizzes are the other type of challenge supported in Sifu. Challenges contain all information and necessary files for the presentation of the task to the player as well as its evaluation by the automated assessment module and hint generation by the artificial intelligence coaching module. Although challenges can only be accessed through rooms, a pre-association to a room is not mandatory. Challenges left disconnected are randomly selected for duel rooms when these are started. Any challenge can reward the player on completion, independently of the room.

**Hint** belongs to a challenge and defines the name, description, and cost (in coins) of the hints generated by the intelligent coach, according to its priority in the ranking of secure coding guidelines, as presented in Gasiba et al. [5]. Actual hints are generated on players' request, and they can opt to buy or not the hint.

**Leaderboard** holds the name, sorting metric (e.g., points and coins), context (global or room-scoped), and reset interval of the leaderboards. Being on top-3 of a leaderboard awards the player a medal at each reset.

**Reward** is a virtual item given to a player for completing a room or challenge or leveling up. SifuV2 includes four types of rewards, namely coins, experience points, badges, and access codes. For the first two, an amount should be set.

**Question and Answer** enable players to submit clarification requests about challenges and administrators to answer them, respectively.

## 3.2 User Interface

The user interface (UI) is a single-page web application developed in Vue 3 with TypeScript, using Tailwind CSS [6] – a utility-first CSS framework packed with several classes that can be composed to build any design directly from the markup. An additional free and open-source Tailwind CSS component library – daisyUI [10] – has been applied to obtain a more characteristic design line. The UI colors, with dark and light themes, follow the company's brand guidelines. Non-authenticated users share the views for registration, email verification, request a password reset, reset password, and signing in. These pages are identical, containing a dojo background, a light/dark theme switch on the screen's bottom-left, and a centered card with the corresponding form. Authentication/authorization is based on access and refresh JSON Web Tokens (JWTs); the former is part of the managed state, whereas the latter is stored in local storage. The global state is managed through Vuex [1], a state management pattern. The library serves as a centralized store for all the components in an application, with rules ensuring that the state can only be mutated predictably.

Logged-in users are either administrators or players, each having its separate SifuV2 environment. The administration side works similarly to a content management system and, thus, has much in common with the characteristic UIs of those systems. A top navigation bar with a togglable menu on the left, the notifications icon, and the user avatar on the right. The content area has a paginated data table with an associated search box (right) on resource listing views, while the details view has the associated resource form. The administrators set up all the content available to the players, including the creation of the rooms, the association of challenges to them, and the definition of rewards delivered on the successful completion of such challenges. Moreover, they are also able to consult the submissions, profiles, leaderboards, and all player activity, as well as to clarify doubts sent by players about a challenge. Figure 1 shows the Activity Log view (i.e., listing view of the events of Sifu v2 users) after clicking the zoom-in button to check the details of an evaluated submission.

The player's dashboard consists of a grid of cards corresponding to rooms. Each card contains the room name and description, an indication of the status relative to the authenticated user, and deck-like visualization of the avatars of at most three randomly selected users who are active in the room (with an indication of the total active users in the room). The player can search a specific room using the search box and hide/show open, closed, completed, and locked rooms. One distinctive aspect of the player environment is that the navigation bar is located on the left rather than on top. This navigation bar can be collapsed to prevent distraction and give extra space.

The Challenge Solving view in Figure 2 has the look and feel of a traditional (simple) code editing application. On the left, the workspace files are presented as a file tree. On the bottom is a simple console emulator where the learner can run several predefined commands and see their outcome (e.g., `submit` to send code for evaluation). The content area has a code

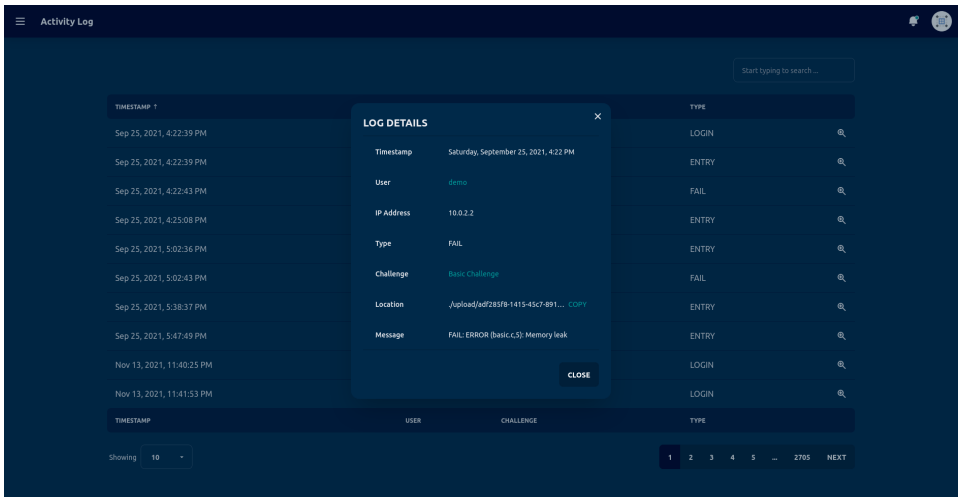


**Figure 1** Activity Log view on the administrator panel, with details of an evaluated submission opened in a modal box.

editor based on Monaco Editor [7], the editor that powers Visual Studio Code, displaying the contents of the active file and tabs for other opened files. On the top of the screen are buttons (from left to right) to change editor settings, report the challenge, reset workspace files, and submit the current files for evaluation. A vital component of this view is the Sifu Master. This animated avatar interacts with the player, providing guidance through hints (when explicitly requested) or presenting the UI tour. The avatar is a CSS3 animated SVG, which can be moved to any position on the screen, with several animations executed depending on the action performed, including looking right/left, blinking right/left eye, waving right/left arm, boiling hat, talk, panic, greeting with the arm, celebrate, angry, and wind on beard and mustache.

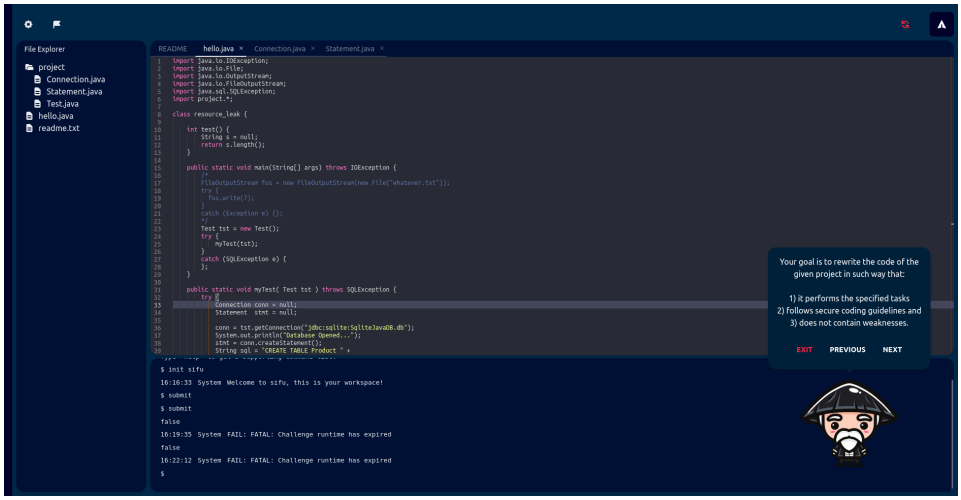


**Figure 2** Challenge Solving view on the players environment.

## 4 Conclusion

Cybersecurity awareness is more and more inevitable in this digital world. The need for professionals with the required knowledge and skills to defend against cyber threats is a top priority in big companies and any digitalized company.

This paper presents the second version of Sifu, a re-design of a cybersecurity open-source system with automated assessment and coaching into a gamified web-based cybersecurity training platform. In addition to gamifying the platform, SifuV2 implements the server-side to adhere to more scalable, interoperable, and flexible web development standards and a new user interface with a cleaner, more attractive, interactive, and independent design. The changes to the interface reflect the author's experience in the field and the design of gamified platforms.

We expect to conduct an online open experiment to evaluate this platform's usability and learning effectiveness in future work. These aim to demonstrate that this platform can improve the cybersecurity awareness of participants while having a smooth and engaging experience.

## References


1 Vue JS Community. What is Vuex? – Vuex, 2023. Accessed on May 2nd, 2023. URL: `https://vuex.vuejs.org`.

2 Ericsson. CodeChecker, 2023. Accessed on May 2nd, 2023. URL: `https://codechecker.readthedocs.io`.

3 Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, 3(1):24, December 2020. `doi:10.1186/s42400-020-00064-4`.

4 T. Espinha Gasiba, K. Beckers, S. Suppan, and F. Rezabek. On the requirements for serious games geared towards software developers in the industry. In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, pages 286–296, Los Alamitos, CA, USA, September 2019. IEEE Computer Society. `doi:10.1109/RE.2019.00038`.

5 Tiago Gasiba, Ulrike Lechner, Jorge Cuellar, and Alae Zouitni. Ranking Secure Coding Guidelines for Software Developer Awareness Training in the Industry. In Ricardo Queirós, Filipe Portela, Mário Pinto, and Alberto Simões, editors, *First International Computer Programming Education Conference (ICPEC 2020)*, volume 81 of *OpenAccess Series in Informatics (OASIcs)*, pages 11:1–11:11, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. `doi:10.4230/OASIcs.ICPEC.2020.11`.

6 Tailwind Labs. Tailwind CSS, 2023. Accessed on May 2nd, 2023. URL: `https://tailwindcss.com`.

7 Microsoft. Monaco – The Editor of the Web, 2023. Accessed on May 2nd, 2023. URL: `https://microsoft.github.io/monaco-editor/`.

8 Pallets. Welcome to Flask, 2023. Accessed on May 4th, 2023. URL: `https://flask.palletsprojects.com`.

9 SonarSource SA. SonarQube, 2023. Accessed on May 2nd, 2023. URL: `https://docs.sonarqube.org/latest`.

10 Pouya Saadeghi. daisyUI – Tailwind CSS Components, 2023. Accessed on May 2nd, 2023. URL: `https://daisyui.com`.