Indian Journal of Science and Technology, *Vol 8(7), 642–649, April 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8i7/67760

Learning Cyber Security Through Gamification

K. Boopathi[1]*, S. Sreejith[1] and A. Bithin[2]

[1]Department of Computer Science and Application. Amrita Vishwa Vidyapeetham University, Amritapuri, India; boopathi@boopathi.me, sreejiths.sasikumar@gmail.com
[2]Department of Cyber Security, Amrita Vishwa Vidyapeetham University, Amritapuri, India; bithin2007@gmail.com

Abstract

Objectives: Introducing gaming approach in the jeopardy round of InCTF (Indian Capture the Flag). **Methods**: Present Jeopardy round of InCTF can be compared as take-away assignments, where participants are given set of questions to solve, this is aimed at testing their knowledge in various computer security concepts. To make jeopardy round more attractive and motivating to the students we introduce a gaming approach to it. A game is developed which is divided into various levels and at each level the knowledge of students in Cyber security concepts is tested. Our design will help others to host jeopardy round CTF and get maximum learning outcome from the students. **Findings**: Security competition like CTF (Capture the Flag) are effective tool in providing computer security training. Conclusion: Gaming approach in Cyber security education will be a big step forward in training more students in computer security and create a secure online world.

Keywords: CTF, Cyber Security, Education, Gamification, Jeopardy

1. Introduction

Based on the defacement statistics of Computer Emergency Report Team (CERT) from Jan 2014 to Oct 2014[1], large number of in domains has been compromised. The figure 1 gives an overview of statistics on the number of domains that have been compromised during this period. This alarming rate of incidences has made us to think whether our software developers are well equipped with knowledge on various computer security concepts. The lack of security experts in India is also a reason behind this increasing number of computer security breaches in our country. This can be avoided by revising Indian curriculum2 at graduate and undergraduate levels. Based on the National Cyber security policy, there is a need of 500000 security professionals in the next 5 years[3]. This need can only be satisfied if there is an efficient training methodology like CTF[4] security competition where the learning is happening in a competitive environment.

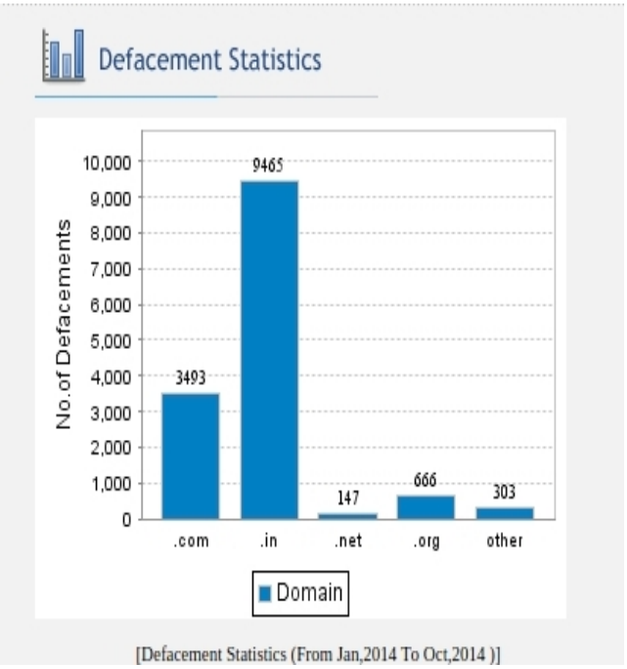

Figure 1. CERT-In Defacement Statistics (From Jan 2014 - Oct 2014).

**Author for correspondence*

InCTF[5] is one such CTF[4] contest conducted in India. But InCTF[5] is different from other CTF[4] contest as it contains three rounds. They are3 learning round, jeopardy round and interactive round.

1.1 Learning Round

This round mainly focuses on introducing some important concepts of Cyber security. Tutorials related to various concepts like Binary exploitation, Reverse engineering, Forensics, Web application security and application security are uploaded and the participants need to use that tutorial to understand these concepts. No evaluation is involved in this round because its only aim is to introduce various Cyber security concepts to the participants. Concepts learned from this round are tested in next round.

1.2 Jeopardy Round

Jeopardy round is testing the knowledge of the participants based on the computer security concepts introduced in the learning round by giving a set of questions to solve. This method lacks the interaction as this is similar to writing assignments. So in order to make this round more attractive and motivate students, we are introducing a gaming approach. Here Cyber security concepts will be introduced through a game which is divided into various levels. Each level introduces various concepts related to Cyber security. The game is divided into four levels with each level testing the knowledge of participants in various concepts of Cyber security. Each level is divided into five parts and new levels will be unlocked once they complete any three parts from each level. First level tests the basic programming skills of participants by giving some basic programming puzzles. In the second level, participants will be tested in web application security concepts like SQL injection attack, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) and file upload vulnerabilities. In the third level, participants will be tested in application security concepts like binary exploitation, buffer overflow, heap overflow and format string attacks. In level 4, participants will be tested in reverse engineering and forensics concepts like file system forensics, memory forensics, Android forensics, network forensics, botnet detection and root kit. This approach will bring back the much needed excitement and motivation needed for the participants.

1.3 Interactive Round

The main aim of this round is to apply the concepts of Cyber security in real word scenario. For that a virtual image is created by deliberately including some vulnerable applications and each team will be given a Virtual Box image or OVF file. Each team is getting the same copy of virtual image as other teams. Each team need to understand the vulnerability in the applications and using that they need to attack other teams and also defend their own system from security attacks of other teams. First a unique flag will be placed in each team's machine and it is done by the game server. Game server is an important component in this round. Planting flags on each team's machine, monitoring the services running on each team's machine and awarding points to teams are some of the main functions of game server. If a team successfully managed to attack other team, flag will be captured and submitted to the game server. After analyzing the flag, game server will award points to the teams in the form of attack and defense points. Attack points are the points that are given to a team if they successfully managed to attack other team by exploiting the vulnerabilities in the application and the defence points are given if they successfully managed to defend their system from the attacks of other teams. Each team's ranks will be shown in the scoreboard with attack and defence points.

In the remaining part of the paper, Section 2 explains the related work which gives an overview of some of the competitions similar to InCTF[5]. Section 3 gives an overview of the game architecture and explains how it can be introduced to make the current jeopardy round more attractive and fun to the participants. Section 4 explains technical details involved in the design of registration portal, game flow diagram and CTF challenge or problem classification. Section 5 gives detailed explanation about various learning outcome for the students after participants in the contest. Section 6 gives conclusion.

2. Related Works

There are various security competitions conducted worldwide. InCTF[5] contest is one such event conducted in India. The main goal of this event is to teach Cyber security concepts effectively.

2.1 iCTF (International CTF)

This contest is organized by the department of computer science University of California, Santa Barbara every year[6]. Their main goal is to enhance the security knowledge of the participants in effective manner. They usually conduct attack-defense style CTF where each team need to attack other teams by exploiting the vulnerability and defend from other attacks. The iCTF framework explains the requirements in conducting CTF and how to configure iCTF framework to conduct our own CTF contests.

2.2 picoCTF

Another hacking competition conducted at United States aimed at teaching security concepts to the high school students7. They will make use of gaming approach to teach security concepts to the students. This method can be adopted in InCTF[5] and modified based on how effectively we can educate our Indian college students with gaming approach.

2.3 rwthCTF

Popular hacking competition organized by the RWTH Aachen University every year8. Another CTF competition aimed at teaching the security concepts to the end users. Because of its poor documentation, the setup of rwthCTF is little known to the users.

These CTFs are international CTFs and high standard, these kind of competitions are hard for Indian students to compete, so we came up with a solution to ease Cyber security education in InCTF[5] so that Indian students can learn the security concepts without any fear of participating in it.

3. Architecture

Gamification is a good approaching in educating students, CTF competitions are trying to adopt this to make its outcome very effective. InCTF5 is trying to use this methodology to teach Cyber security in coming years. Because gaming is always best when it comes to entertainment and excitement9. Figure 2 explains an architecture that shows how the gaming interface can be developed with the help of various technologies.

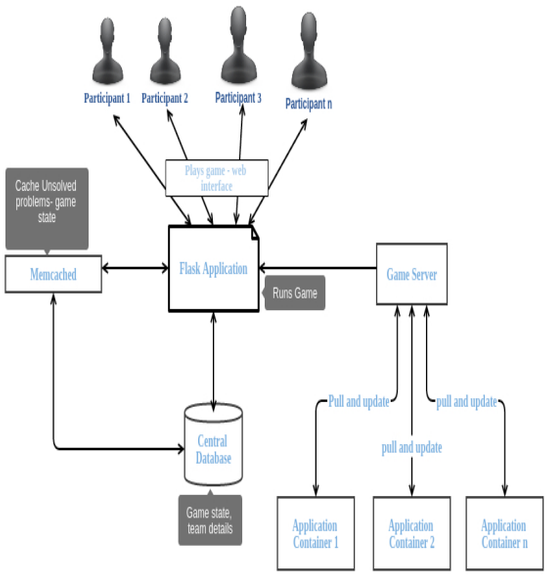

Figure 2. InCTF architecture diagram.

3.1 Central Database

This database is implemented in mongo DB, which is a NoSQL database. We have chosen in order to increase the speed of the website. The main functions of central database is to store the details of the team members, problems, game status and the scoreboard status.

3.2 Memcached

This is a distributed memory caching technology which is used to reduce the number of request send to the central database. Large number of teams will be accessing the gaming environment at the same time. So thousands of request will be send to the central database and there is a chance that the system might crash. To overcome this problem we will be making use of this memcached technology. Using memcached all the unsolved problems from the central database is cached and loaded from memcached instead of loading it from central database. Only the status of the solved problem is kept in the central database. So next time when a team tries to access any unsolved problem, that will be loaded from memcached rather than going to the central database.

Only the important requests like updating problem status and scoreboard status will be send to the central database.

3.3 Flask Application

It is a popular python micro framework, used to develop lightweight web application because it keeps the core simple and supports extension. Flask uses Werkzeug WSGI (Web Server Gateway Interface) and Jinja2 template engine. Jinja2 template engine adds sandboxed execution for security reason.

4. Contest Design

4.1 Registration

Participants from Indian universities are only allowed to register, once the participants completes their individual registration, confirmation email will be send to them. They need to confirm their account by clicking the link sent to them by email. On activating the participant's account, they can form the team with same college members. Minimum of 3 and maximum of 5 members are allowed per team with a coach.

4.2 Publicity

We do publicity through various social Medias like Facebook, Twitter, WhatsApp, blogs. Sending posters to colleges, Contacting universities and teachers, Mailing list and Local newspapers in all major cities and area where there is lot of colleges.

4.3 Game Design

The game is divided into 4 levels with each level testing knowledge of the student about various concepts of Cyber security. The difficulty level increases as the level increases. Teams need to solve 3 parts in each level to unlock new levels. In first level, a boy found a hidden box from his house. He will open that box by solving a set of challenges. After opening that box a robot comes out of that box and become friend with that boy and agrees to help him to solve the remaining challenges as the game progresses. This level test the basic programming skills of participants by giving various programming puzzles. This is the scenario in level 1. In level 2, boy and robot reach a place that is not familiar to them and suddenly they lost a way back to their home. They found a map from that place by solving some challenges and discover the way back to their home. This level test various concepts related to web application security. This is the scenario in level 2. In level 3, boy gets an invitation for participating in a Hackathon competition. He needs to get eligibility pass by solving a set of challenges. This level tests various concepts related to application security. This is the scenario in level 3. In level 4, after getting the eligibility pass he will participate in Hackathon competition. There some set of challenges will be given and need to solve it to win the competition. This level tests various concepts related to Reverse engineering and Forensics. This is the storyline of the game. Figure 3 shows the execution flow of the game and the various concepts tested in each level.

4.4 Problem View

There are two ways users can view the problem. One way is through game and another way is through normal text based view. In game, participants can view the problem by moving into the position by using arrow keys in keyboard through game and it is shown in the figure 4. Another method is through normal problem viewer window. In this method, participants can simply select the problems and it will be shown in a separate window. Problems will be shown in new window and simply submit answer for the problem. Figure 5 lists the solved and unsolved problems.

4. Discussion on Concepts Taught

Various concepts taught during Jeopardy round through our gaming approach are discussed here.

5.1 Level 1

Part 1 - Puzzle to print a sequence of characters in some order.
Part 2 - Puzzle to print the numbers without using any loops.
Part 3 - 1-D and 2-D array puzzles.
Part 4 - String operations puzzles.
Part 5 - Puzzle related to printing Pascal's triangle.
These are all the concepts tested in level 1. In level 2, concepts related to the web application security will be introduced. This level will test the knowledge of participants in web application security.

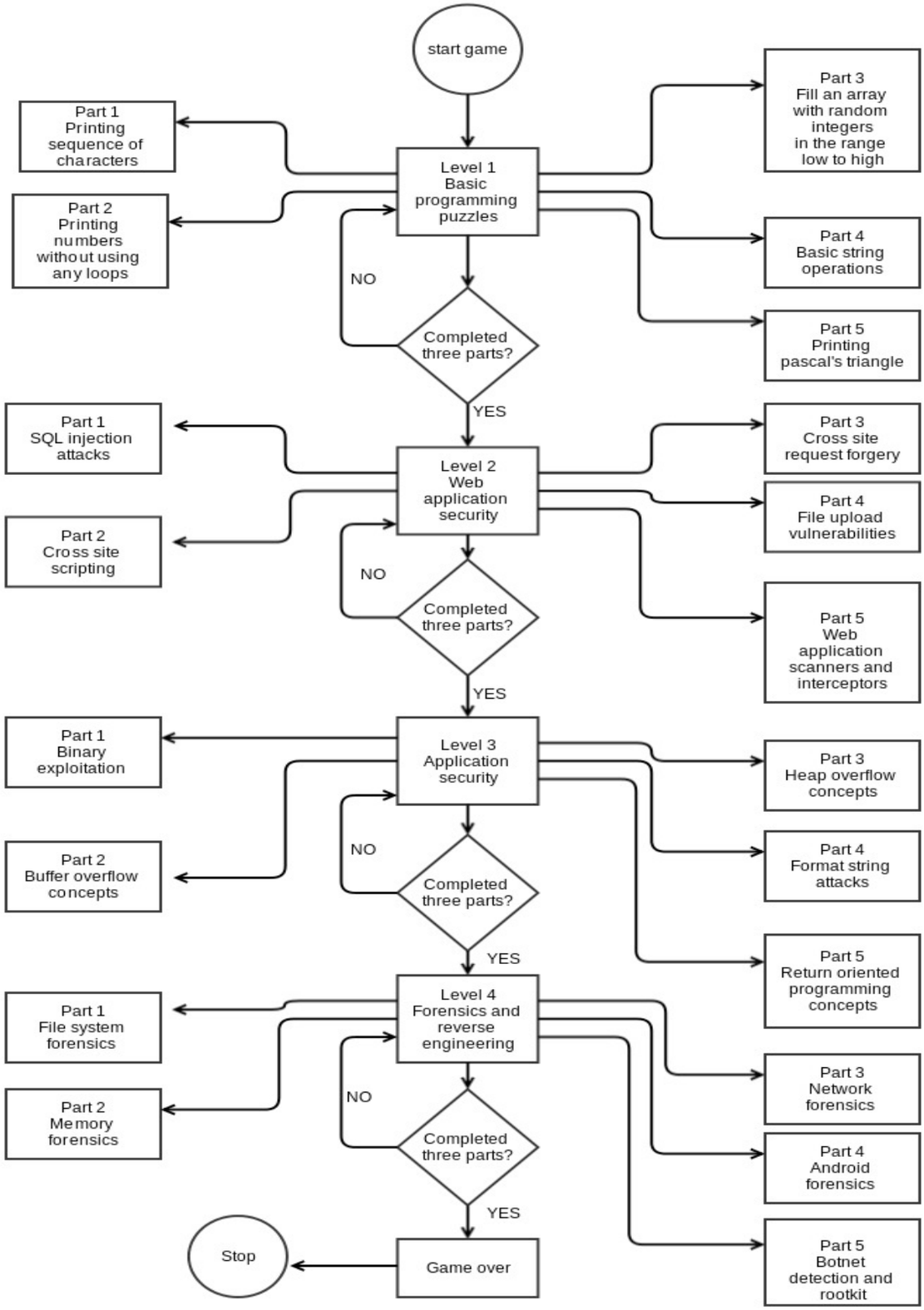

Figure 3. Game flow chart.

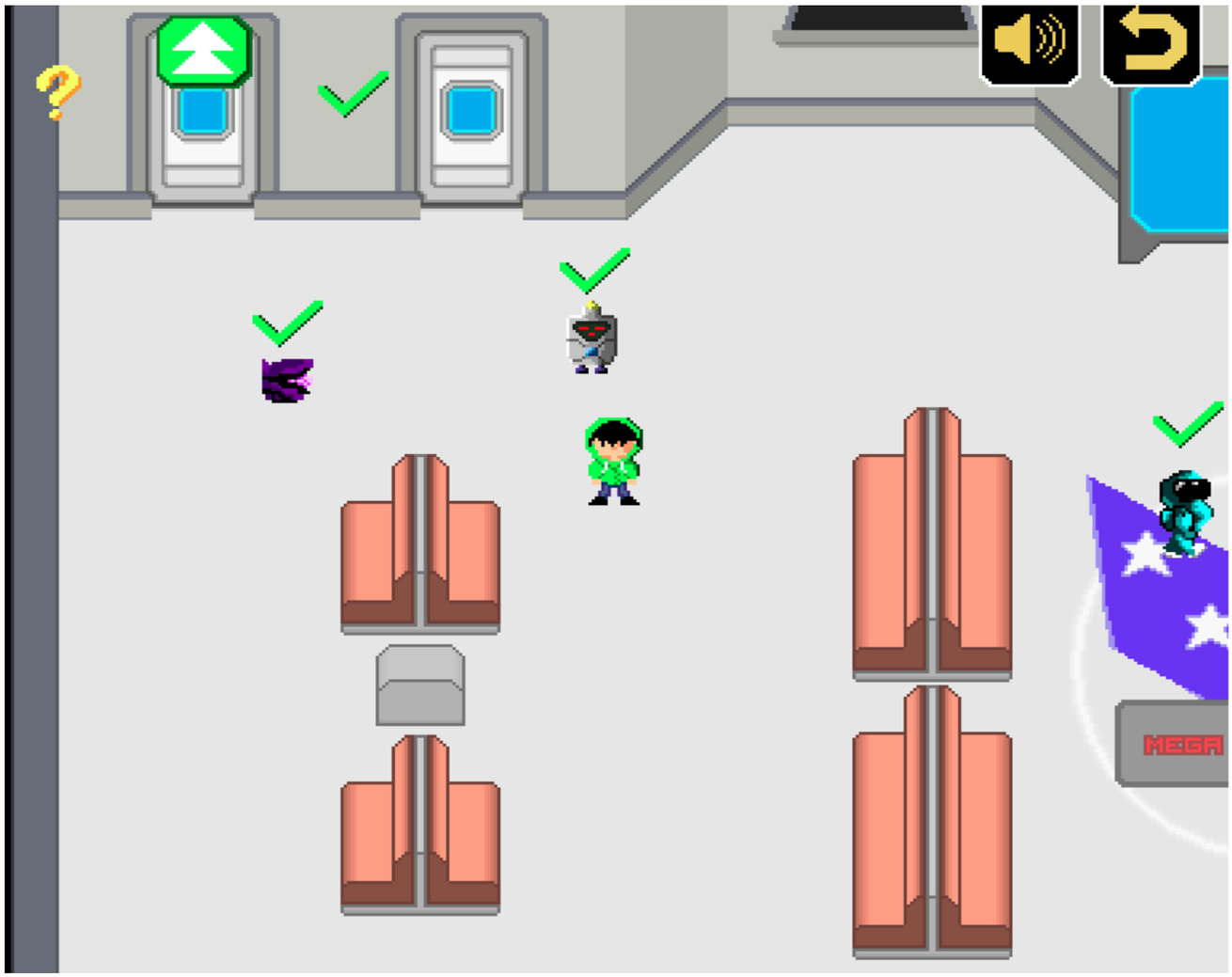

Figure 4. Game environment.

5.2 Level 2

Part 1 - SQL injection attacks
Part 2 - Cross Site Scripting (XSS)
Part 3 - Cross Site Request Forgery (CSRF)
Part 4 - File upload vulnerabilities
Part 5 - Web application scanners and interceptors
These are all the concepts tested in level 2. In level 3, concepts related to the application security will be introduced. Participants will be tested in various concepts of application security.

5.3 Level 3

Part 1 - Binary exploitation
Part 2 - Buffer overflow
Part 3 - Heap overflow
Part 4 - Format string attacks
Part 5 - Return oriented programming concepts (ROP)
These are all the concepts tested in level 3. In level 4, concepts related to the Forensics and reverse engineering will be introduced and the participants will be tested in the various concepts of this topic.

5.4 Level 4

Part 1 - File system forensics
Part 2 - Memory forensics
Part 3 - Network forensics
Part 4 - Android forensics
Part 5 - Botnet detection and rootkit
These are all the concepts tested in level 4.

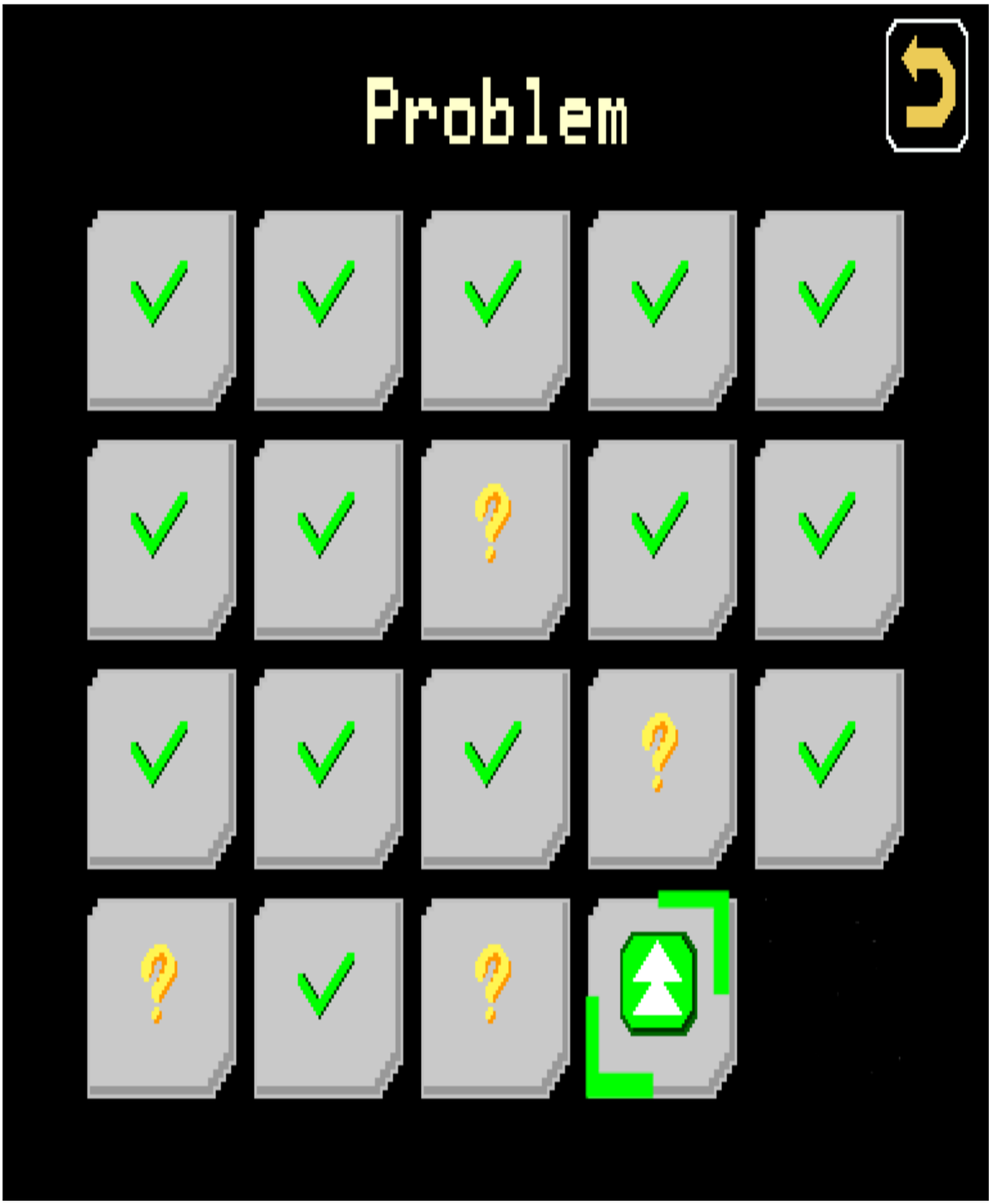

Figure 5. List of solved and unsolved problems.

6. Conclusion

'Learning for fun' is an effective approach for Cyber security education. It will take students great forward in training more students in computer security. This approach keeps the students motivated and Jeopardy round will be able deliver more learning outcome.

7. References

1. Defacement Statistics of Computer Emergency Response Team India (CERT-In); 2014 Jan-Oct. Available from: http://cert-in.org.in/
2. Kumar CRS. A review of cyber security curriculum in indian context. Department of Computer Engineering, Defence Institute of Advanced Technology, Girinagar, Pune; 20104 Sep.
3. National Cyber Security Policy; 2013 p. 4. Available from: http://deity.gov.in/content/national-cyber-security-policy-2013-1.
4. List of CTFs Time. Available from: https://ctftime.org/
5. Joshi A, Ramani V, Murali H, Krishnan R, Mithra Z, Pavithran V. Student centric design for cyber security knowledge empowerment. Amrita Centre for Cyber security; 2012 Jan.
6. Vigna G, Borgolte K, Corbetta J, Doupe A, Fratantonio Y, Invernizzi L, Kirat D, Shoshitaishvili Y. Ten Years of iCTF: The Good, The Bad, and The Ugly. Barbara: University of California in Santa; 2014 Aug.
7. Chapman P, Burket J, Brumley D. PicoCTF: a game-based computer security competition for high school students. Carnegie Mellon University; 2014 Aug.
8. rwthCTF. Available from: http://ctf.itsec.rwth-aachen.de/
9. Kannan M, Geetha M, Sujatha J. An analysis between traditional and motion detection game – using ICT techniques. Indian Journal of Science and Technology. 2014 Dec; 7(12):1956–62.