Raising Cybersecurity Resilience With CyberSmart Trivia

1st Dhani Kataria
Dept. of Electrical and Computer Engineering (MTIS)
University of Victoria
Victoria,Canada
dhanikataria@uvic.ca

2nd Hailay Teklemariam
Dept. of Electrical and Computer Engineering (MTIS)
University of Victoria
Victoria,Canada
haitek@uvic.ca

3nd Shreya Goyal
Dept. of Electrical and Computer Engineering (MTIS)
University of Victoria
Victoria,Canada
shreyagoyal@uvic.ca

4thAnuinder Sekhon
Dept. of Electrical and Computer Engineering (MADS)
University of Victoria
Victoria,Canada
anuindersekhon@uvic.ca

5thVatsala Arora
Dept. of Electrical and Computer Engineering (MADS)
University of Victoria
Victoria,Canada
vatsala09@uvic.ca

***Abstract*—The rapid advancement in technology has led to the emergence of web-based solutions in the fields like banking, data storage, and customer service. This has led to a rise in cybercrimes such as ransomware, cyberbullying, and phishing each year which are affecting both individuals and large organizations. With cybercriminals continuously working on creating new attack vectors, it has become important for organizations and individuals to become aware of the practices of Cybersecurity. Since most personal data breaches occur due to carelessness and lack of knowledge, therefore, the knowledge of the basics of networks and network security can help individuals in recognizing if they are becoming the victims of cyberattacks or not. That is why, the first step in learning any new technology is always to understand the basic fundamental concepts. To improve the learning experiences while making it easier to grasp new concepts in an engaging way, our team (Security Knights) has adopted the technique of gamification. In order to gamify the process of learning about cyber security, we have developed a web-based game called 'Cyber Smart Trivia'. This game is adapted from the "Who Wants to be a Millionaire" Challenge with the focus on teaching a new concept with every question.**

***Index Terms*—Cybersecurity, Information Security, Millionaire Quiz, Gamification, Security Awareness, Adobe Captivate, Web Vulnerabilities, Section 508, WCAG, HTML5, Mobile Gestures**

I. WHY GAMIFICATION IS IMPORTANT?

Students, youth, adults, and even engineers, all are caught up and influenced by games in general. Gamification is the incorporation of design aspects and ideas into non-game situations such as education, marketing, and staff training to make them more engaging. It can be a powerful tool for learning and skill development. Research [1] shows that gamification could be considered a vital tool for creating sustainable material for higher educational institutions by improving underline motivation and performance. It provides a structured and interactive environment where individuals can acquire knowledge, practice skills, and receive immediate feedback. By presenting information in a game format, it can make complex or mundane subjects more accessible and enjoyable to learn. Gamified learning includes aspects like high scores and virtual rewards which increases the players' engagement by motivating them with the achievements they earn. This is because people like to feel and see that they're actually making progress. Learning by playful means helps in better information retention which is yet another reason which shows why gamification can be considered as an essential part of any learning. Our game tends to target all these essential components of gamification, making the learning process of information security a fun and exciting journey for the user.

Gamification has the potential for improving the enjoyment of activities, increasing motivation to perform desired actions, and driving desirable behavior. It has proven to be a very valuable strategy in different areas, including education, training, healthcare, marketing, and employee involvement, which ultimately results in better experiences for individuals and organizations. Keeping all this in mind, we designed a game that not only hooks the users but also teaches them the basics of security such as phishing, account security (passphrases, MFA), device security, and IoT security.

II. TOOLS USED FOR THE DEVELOPMENT

The tool to be used for the game development is "Adobe Captivate" which is a kind of Digital Learning Solution by

Adobe [2]. This is a GUI-based tool that allows the creation of e-learning content in the form of a quiz, online course, etc. The tool allows the creation of content in the form of interactive slides. The creators can easily incorporate other media such as images, videos, etc. into the slides to make the overall experience more immersive. They can use this tool to build different types of e-learning courses such as software simulations, compliance courses, assessment courses, and soft skill courses. The game should be web-based and Adobe Captivate allows the creator to author HTML5-based content of it without the need for any programming. Such ease of use has made this tool quite popular among large enterprises and it is no surprise that companies like Amazon, J.P. Morgan, and Boeing are using it for their Learning Management Systems. This tool also has some amazing features such as the creation of virtual reality games, interactive videos, automatic device previews, and PowerPoint to responsive learning content.

Anyone can download Adobe Captivate as long as they have the following in their systems: Microsoft Windows (Windows 7/Windows 8.1/Windows 10 or later) with a minimum of 4 GB of RAM or Mac OS X v10.12.3 (or later)/iOS 10.2.1 (or later) and 10GB of available hard-disk space for installation. It would be better to have additional free space during installation. After this, they just have to create their ID, download and install the tool to run it.

III. GAME INTERFACE

This section of the report will describe the various components of the game. The details have been divided into various subsections highlighting the game content and other features of the GUI which adds to the overall dynamics of the game. The motive of this project is to spread security awareness playfully so that users can grasp the much-needed cyber security concepts. Therefore, the dynamics of the game are designed in a way such that it provides a captivating and intellectually stimulating experience to its players.

A. Interactive UI and Audio

Our game begins with an interactive UI and game sounds to keep the user hooked from the beginning. The Figure 1 shows the image of the introductory screens where we are introducing the audience with the game name and giving them time to prepare themselves before they begin playing. In the attempt to keep the game simple yet interactive for all age groups (youth-seniors), we chose the theme based on ”Who wants to be a millionaire” [15]. For creating a more immersive experience, the game includes different sound effects in different instances. Moreover, for each of the questions, audio samples can be added to the game and the corresponding options for the players. Such sound effects will create an atmosphere for users which makes the game more fun to play with.

B. Features and Ideas

After beginning the game, the user is asked their first question with the four relevant options to choose a right answer from them. The snapshot of the view visible to the user is

Fig. 1. Introduction screen available to player

shown in Figure 2. One of the options has the right answer while the rest three of them are wrong. The user also needs to answer the question within a time frame in order to avoid copying answers. As shown in Figure 3, every question also has a relevant Hint and Idea icon which when clicked will show some hints that can guide the user in answering that question. After selecting an answer the game asks the user for re-confirmation if that is their final choice for submission or not. After confirmation by the user, the game reveals if the answer is right or not.

C. Type of Questions

The game's questionnaire covers various aspects of information security such as phishing, password security, device security, and IoT security. These topics are just the exemplary areas but the actual game includes a broad spectrum of questions covering multiple domains starting from physical security to implementing security at both network and software levels.

The questions are not just from the perspective of a potential victim, rather, they cover the viewpoint of both an attacker and a defender. This allows the players to think about how the attackers usually target their victims and how they can avoid getting exploited. Further, the underline focus of the game is to aware of the users regarding cyber-attacks that are more prevalent in the IT world. Apart from teaching the users about various attacking and defensive techniques, the questionnaire also tests the players regarding the known best practices. Such knowledge is critical because there are always multiple ways to solve a security problem, however, there is only one best choice that can ensure the security posture of the underlying infrastructure.

D. Education Contents

The main motive for designing this game is to make people aware of the importance of cybersecurity. Therefore, the major aspect of the game is to educate the players such that they can realize and exercise best security practices in their day-to-day routine. Whenever the user answers any question, the game provides a brief regarding why the correct option is correct and other options are wrong. This is designed to improve the decision-making for the players in case they encounter

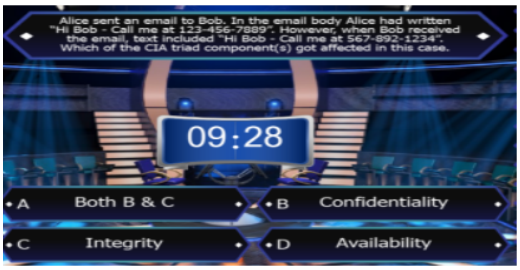

Fig. 2. Sample question with options and timer

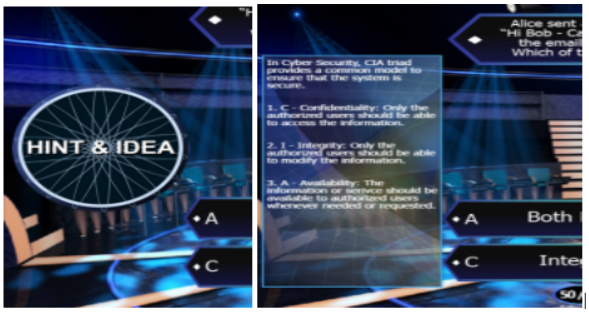

Fig. 3. Hint and Idea flip card for assistance

some security incident in the future. As mentioned previously, though the game provides some context or hints for most of the questions. The knowledge of these terms will not only educate the users, rather it will provide a base for normal users to perform further research on the security concepts. Also, the focus of the questionnaire is to teach users how they can recognize potential attacks and if they encounter such attacks, then, how can they prevent or mitigate them to reduce the involved risks. The Figure 4, represents the type of explanations the game provides after each answer.

E. Exciting Rewards

The designed game has been divided into several question levels and currently has fifteen levels. Each level in the game represents a milestone in terms of both difficulty and prize money. As the player keeps playing, the concept of cybersecurity understanding and the rewards increases. The questions in the game are arranged in a progressive difficulty way, starting from the easy ones and becoming more informative as the game progresses. The first question is at the lowest level which is pretty straightforward and simple as compared to the more challenging questions that follow. The reward associated with this question is also the smallest one as compared to other rewards. The first question is the starting point from which the player can potentially increase their winnings. As the player answers more questions correctly advancing through the game, answering questions becomes harder and the rewards increase, tempting them to keep playing the game and eventually increasing their knowledge of cybersecurity.

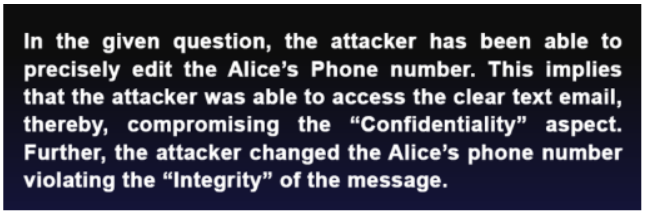

Fig. 4. Explanation given after every right/wrong answer

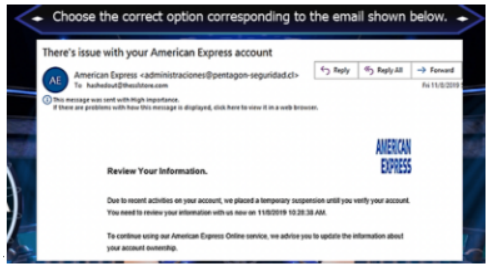

Fig. 5. Types of Questions: Image Based

Fig. 6. Types of Questions: Drag and Drop

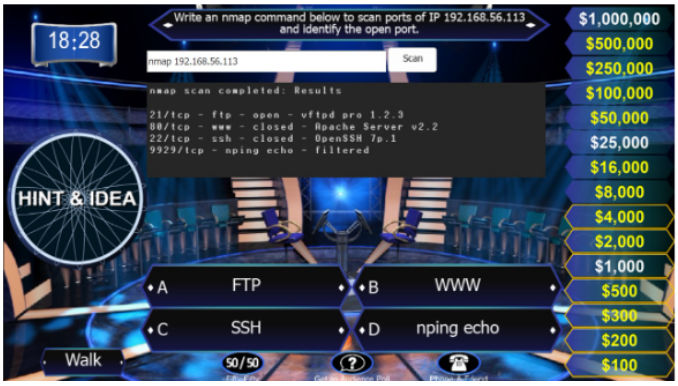

Fig. 7. Types of Questions-Code Simulation

F. Question Format

As the questions in our games are scenario based, the questionnaire includes a variety of formats. We have designed the questions in the form of text, images, or videos portraying a simulation of potential attacks. Moreover, we have drag and drop type format as well as code simulation type questions. The drag-and-drop questions allow the users to place the correct options with the corresponding choice by dragging the option to the provided spaces. We have also provided the option to undo and reset these types of questions so that the users can revert to a wrong selection or reset and do the whole question again. In the code simulation-type questions, the user must enter the code or command to answer the question. If the user enters the wrong code, the user will get 'Wrong Command' on the screen. However, if the user writes the correct code, he earns the reward and moves on to the next question. These different formats make the game easily relatable to real-life situations and help the player learn and adapt in a user-friendly manner while providing the users with a practical perspective. The Figure 5, Figure 6, Figure 7 are the snapshots of all the types of questions used in the game.

G. Survival Lines

In our game, we are offering three survival lines to the users:

- Fifty-Fifty: In this Survival Line, we remove two out of the four options which are incorrect. The user is left with only two options to choose from where only one is correct. This gives the user a 50/50 chance of selecting the correct option which increases the chance of selecting the correct answer.
- Poll-the audience: The Poll-the-audience option works by providing the user with varying probabilities for each option. The game logic works by assigning the highest probability to the correct answer to make the game more interactive and engaging for the user.
- Phone-A-Friend: This survival line presents an amusing way to provide the user with the correct answer. Our game logic simply gives the user the correct answer upon using this survival line by playing a formerly prepared audio clip.

The Figure 8, Figure 9, Figure 10, Figure 11 show the types of survival lines in the report.

Fig. 8. Survival Lines available to the user

Fig. 9. Survival Line- 50/50

Fig. 10. Survival Line- Audience Poll

H. Walkover Feature

The walkover feature allows the player to quit the game after reaching certain checkpoints in the game in case the user wants to leave the game in between. With this option, the user can walk out of the game with the amount he has earned at the checkpoint.

I. Dynamic Orientation

Our game supports dynamic changes of orientation for the comfort of the user to play the game in landscape and portrait modes. This feature ensures that the player can play the game in whichever orientation they prefer on their devices.

IV. ACCESSIBILITY

This game has been developed with the aim of educating a wider range of people, so we have considered the accessibility

Fig. 11. Survival Line- Phone a friend

requirement for most of the commonly available platforms during development. These requirements have been implemented in our project taking level AA of Web Content Accessibility Guidelines (WCAG) [4] as a reference. The details regarding the platforms and the WCAG guidelines have been mentioned in the following subsections.

A. Compatible Platforms

This game has been developed with the aim of educating a wider range of people, so we have considered the accessibility requirement for most of the commonly available platforms during development. These requirements have been implemented in our project taking level AA of Web Content Accessibility Guidelines (WCAG) [4] as a reference. The details regarding the platforms and the WCAG guidelines have been mentioned in the following subsections.

B. Compliance with WCAG

The WCAG provides a list of recommendations for creating the layout of the web content so that it can be more accessible to a wide range of the public. In 2012[4], the International Organization for Standardization accepted the WCAG version 2 as an ISO international standard. It defines four principles [4] for websites which are mentioned below:

- Perceivable
- Operable
- Understandable
- Robust

WCAG 2.0 has specified three different levels for guidelines, i.e. Level A, Level AA, and Level AAA [4], in decreasing order of priority. Our project complies with the Level AA of guidelines. The Adobe Captivate provides an in-built feature to generate education content that follows section 508 standards [5] which also apply to the WCAG 2.0 Level AA requirements. This ensures that our game's content follows these guidelines, some of which have been listed below:

- Our project has ensured all the non-text present in our game has a descriptive text alternative.
- WCAG provides flexibility in deciding the orientation of the content i.e. landscape and portrait and our game suits both.
- Our project ensures the visual presentation of the text follows all the ratios specified by the WCAG 2.0 standards.
- Our project ensures that the WCAG 2.0 guideline stating to provide the user a mechanism to control the volume of the audio exceeding 3 seconds has been considered.
- To make this game accessible for people with photosensitivity, we have ensured that there are no flashes per second.

V. PUBLISHING

Adobe Captivate includes a built-in option to publish the developed content as HTML5-based web content. When the user clicks on the publish button, Adobe Captivate generates backend files on the local computer. There are multiple folders and files including script files. The folder named "vr" contains

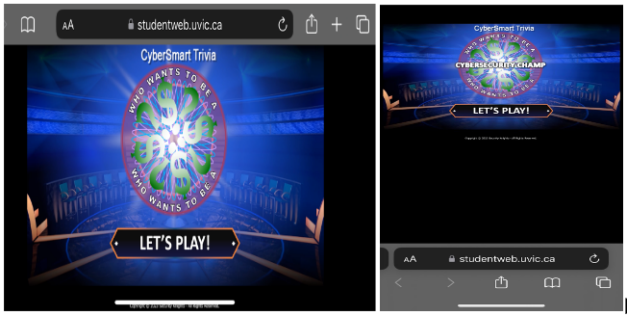

Fig. 12. Different views in which game works

all the video files and likewise, different folders can include other forms of media like images, audio clips, etc. that have been used for building the game. All the generated backend files have been copied onto UVic's Webserver and public access to index.html has been enabled. This way anyone who wants to play the game can play it on the UVic's hosted webpage. Our game can be made accessible on the web. This also includes making the game playable on mobile devices by leveraging the use of touch screens.

The game is designed in such a way that the touch gestures are recognized and working. The users can easily play the game by tapping on their screen and selecting the answers from the given options. The users can easily navigate through the game and explore different elements using this feature. The game can be played in either orientation, landscape, or portrait, whichever seems more comfortable to the user.

The Figure 12 shows the desktop and mobile view of the game published on the UVic's web server.

In addition to hosting on UVIC student web subdomain, the game has been also hosted in Azure cloud. Ubuntu 20.04 virtual machine has been deployed with an Apache HTTP server installed to host the game. Hosting has different advantages such as scalability, flexibility, cost savings, better collaboration, data loss prevention and advanced security. The game can be easily accessed using a URL link and QR code generated specifically for this project. The 13, shows the OQ code for . URL: security-knights.westus2.cloudapp.azure.com

VI. PUBLISHING

Fig. 13. QR code for the game URL link

VII. SECURITY AND PRIVACY REVIEW

The main objective of developing this game is to provide users with learning experience for protecting their data and their organization's security. When users are playing this game, the platform must lead by example for being secured and protected from unnecessary attacks and preserve its reputation. To encourage users to spend more time on getting security awareness, a reward-pointing system database is stored in each account session. Accounts are secured with strong passwords where every time the user visits the individual score can be retrieved.

According to the visitor's level of expertise in information privacy and security, flaws, and vulnerabilities are being probed. Before implementing the game, thorough penetration testing is to be executed. The foremost emphasis is to be given to the development tool, Adobe Captive. Online research on common vulnerabilities and exposures (CVE) could offer knowledge on which versions of the development tools are outdated or patched. From the https://cve.mitre.org/ platform updated database investigation report, vulnerability name CVE-2017-3098 related to the feature Adobe Captivate version 9 and earlier could be exposed to remote execution attack especially in quiz reporting that leads to random read and write files in the server [6]. A new release with an automatic update of Adobe Captive is to be chosen as the hosting and development platform for this project. In addition to the CVE vulnerability database, Open Worldwide Application Security Project (OWASP) foundation guidelines are also to be applied as a benchmark for securing web-based applications [7]. Hosting web-based game applications for cyber security awareness contribute immensely due to ease of access, location, time, and device independence. Even though hosting web-based game applications has various merits and benefits, there are different occasions where users wouldn't adhere to policies and recommendations presented by the owners. This issue could be categorized as malicious intent or security and privacy ignorance. The bad actors could exploit the weakness or vulnerability of the game's front and backend website due to misconfiguration, design, or coding practices. The effect of these flaws is gaining unauthorized access, exposure of sensitive data, or compromising the website's functionality. Website vulnerabilities could be subjected to different types of exploit attacks. Some of these are listed below:

- Cross-Site Scripting (XSS) attacks are performed by injecting malicious code into user input fields. Hence inputs are to be validated with special characters vetted as string text variables.
- SQL Injection is executed to gain unauthorized users' database access by injecting SQL script that reveals the secret data. Validating the user's URL or input field entry would deter or prevent the attack.
- Cross-Site Request Forgery (CSRF) refers to deceiving users into clicking malicious URLs that originated from trusted sources without permission. Avoiding state change

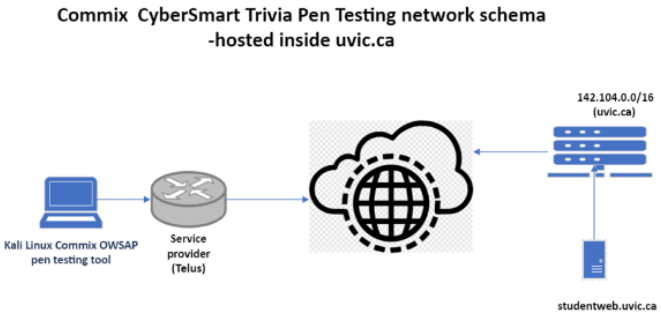

Fig. 14. Commix injection testing against Cybersmart trivia game hosted inside studentweb.uvic.ca

Time	Severity	Type of command Injection attack	Targeted Resource	Status	Est. Duration of attack (s)
00:28:00	Info	Identification	HTTP Cookie header	Not tested	<1
00:28:01	Warning	Heuristic (basic)	HTTP header 'User-Agent'	Not injectable	1
00:52:32	Info	results-based (classic)	GETHTTP header 'User-Agent'	Not Injectable	14,332 (3.98 hours)
01:01:50	Warning	results-based (dynamic code evaluation)			
01:03:53	Info	Blind (time-based)			
04:49:03	Info	temporary directory creation			
04:51:24	Info	(semi-blind) tempfile-based			
04:51:25	Warning	Heuristic (basic)	HTTP header 'Referer'	No Injectable	1
05:15:38	info	results-based (classic)	GETHTTP header 'Referer'	Not Injectable	1,779 (29.65 Min)
05:27:45	Warning	results-based (dynamic code evaluation)			
05:30:28	info	Blind (time-based)			
05:42:37	info	temporary directory creation			
05:45:17	Info	(semi-blind) tempfile-based			
05:45:18	Info	Heuristic (basic)	HTTP header 'Host'	No Injectable	1
06:09:24	Info	(results-based) classic	GETHTTP header 'Host'	Not Injectable	1,233
Same test parameters					20.55 min
06:29:57	Warning	(semi-blind) tempfile-based			
06:29:57	Error		All tested parameters and HTTP headers	Not Injectable	

Fig. 15. Table Summarizing CyberSmart Trivia inside same VLAN Configuration inside Virtual Box

for GET request actions could have the remedies for the attack. Broken authentication and session management take place when a website is not properly implemented with authentication and session management procedures could lead to hijacking or stealing user credentials. File inclusion vulnerability occurs when an attacker includes files from the local file system that trigger arbitrary remote code execution. To exhaust website-related vulnerability attacks, some of the techniques and tools are authentication and authorization, input validation, secure code development practices, regular, audit and updates.

Currently, there are various OWASP-based web application vulnerability penetration testing tools. They can be categorized as freely available open sources and demand paid subscriptions. Some of these tools are namely OWASP ZAP, Burp Proxy, Web stretch Proxy, Session Manager, Commix, and so on. They can be manual or automated through available scripts and programming languages.

Commix is an open-source web application vulnerability testing tool that stands for command injection and exploitation [11]. Commix automates tools to exploit the command injection vulnerabilities which is useful to pinpoint security flows in web applications. It supports attack vectors that target POST, GET, headers, and cookies. In this project, the Cybersmart trivia HTML5 file package has been hosted in the UVIC student web portal. UVIC student web portal is a subdomain of the uvic.ca website where each student is allowed to host specifically allocated web applications. Since the student web portal is part of the UVIC enterprise web server it is highly protected and dynamically secured with extra layers. An unharmful target Commix injection attack was conducted to find the flaw in the embedded Adobe Captivate HTML5 file inside UVIC student web portal. Commix was launched inside Kali Linux security vulnerability testing operating system command line interface [13]. The interactive dialogue version of Commix wizard was initiated to test the flow inside the UVIC subdomain web portal. The following series of parameters were inserted to start the injected process.

- Enter full target URL (-u) ¿ https://studentweb.uvic.ca/ haitek/index.html
- Enter POST data (–data) [Enter for none] ¿
- Enter injection level (–level) [1-3, Default: 1] ¿ 3

The first dialogue command waits for Uniform Resource Locator (URL) the Cybersmart trivia inside the UVIC student web portal. The parameters are for POST data since there is no post-text request data supplied by contested it is left empty or has no parameter. The injection level ranges from 1 to 3 where level is the measure of intensity of the detection phase. The Figure **??** shows the screenshot of the pen-tested CLI output.

The Commix has generated cookies by exchanging data through HTTPS protocol. The output cookie is "('UVicPMember=!vYHnfol85p...AKMpVLFeUw==') "as shown in the figure screenshot from Kali Linux CLI. The Heuristic (basic) tests show that the Cookie parameter 'UVicPMember' might not be injectable. The parameters HTTP headers User-Agent, Referer, and Host are not injectable. Overall hosting Cybersmart trivia inside UVIC web server infrastructure with student web subdomain is highly secured and is immune to HTTP headers injectable attack. The main reason is UVIC has invested in protecting and securing its web server, network, and data with updated software tools, network firewall, application firewall, intrusion detection system, intrusion previous system, and other hidden layered security hardware and applications. This is shown digramatically in Figure 14.

Since UVIC network infrastructure is highly secured plus web services are hosted in a secured version of HTTP protocol with port 443, as expected the Commix simulated attack or pen testing was not successful. The game had been deployed in a controlled environment with unsecured HTTP port 80 as a communication protocol to directly test the vulnerability of Adobe Captivate contests of the game. To conduct this experiment an open-source Apache HTTP server was installed in Ubuntu 22.04 guest virtual machine [14]. The Cybersmart trivia game package was copied into the '/var/www/html' directory. The game URL is http://localIPaddress. The attacker's Commix tool was hosted inside a Kali Linux guest Virtual machine where the victim and attackers were connected through a virtual switch in the same VLAN with IP addresses of 192.168.1.100 and 192.168.1.75 respectively. The outcome of the experiment is summarized in the following table. The server VM and client VM are connected through a virtual switch configured inside Oracle VM VirtualBox Manager hypervisor type 1.

From the OWASP-compatible Commix pen testing, it can be assumed that Cybersmart trivia is relatively secured with the HTTP header parameters test conducted as shown in the Figure 15, even if it is hosted in an unsecured Apache HTTP server with port 80. In addition to basic file access permission configuration inside the Ubuntu operating system and /var/www/html Apache default directory Adobe Captivate's latest version (11 or later) was used to create the web application game. Version 11 has been immune to CVE-2017-3098 vulnerability which exposes remote execution attacks during quiz reporting unlike Adobe Captivate 9 or earlier. Since the game is hosted in the UVIC web server and AWS cloud it reaps the benefit of secured network infrastructure in both cases. On top of that, Adobe Captivated conceals web applications from web attack vectors such as XSS, CSRF, file inclusion, directory traversal, and others.

VIII. MAINTAINABILITY, ACCESSIBILITY, AND MANAGEABILITY

Most cybersecurity-related training and awareness are strict procedural rules that bore with technical jargon and focus on the technical aspects of security and privacy. Adobe Captive is mostly convenient for creating e-learning and interactive media development tools with automatic HTML5 generation capability. The game content can be published in three different ways namely local computer, adobe connect, or adobe learning manager. Users have the option to download, try the awareness on their local computer, or publish into adobe connect. Adobe Connect is Java based web application running on the Tomcat servlet engine [6]. The server duties are access

control, security quotas, licensing, auditing, and management functionalities. It provides transcoding of media files such as Powerpoint presentations and audio. The application server manages requests and content transfer requests over HTTP or HTTPS connection. Adobe Media Gateway integrates Adobe

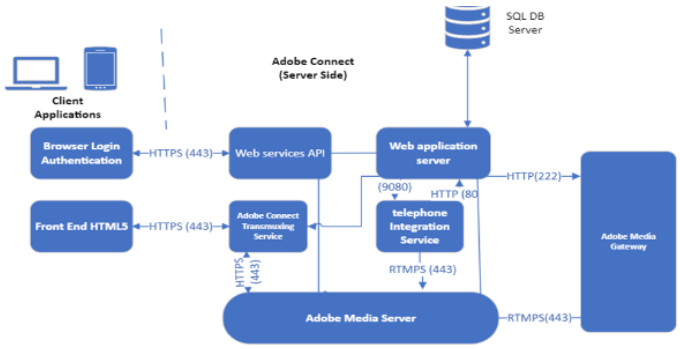

Fig. 16. Data flow architecture of web-based cyber security awareness with Adobe Captive

Connect with Session Initiation Protocol (SIP)/ RealTime Transport Protocol (RTP) setup. This helps phone communication requests from users in playing the game into Adobe Connect spaces. For storing users' details and scoring systems, an embedded database engine inside Adobe Connect is used for reducing the complexity and costs for a stand-alone SQL server [12]. The Figure 16 shows the digramatic represenation of this process. Data flows from client to server or vice-versa. Data communication between the front-end and back-end applications is to be secured. For secure connection across network or internet data flow is secured using encrypted HTTPS (443) protocol instead of unencrypted HTTP (80). Web browser from client-side requests content uniform resource locator (URL) over a secured HTTPS (443) connection. The web server replies requested content through a secured connection. After the response from the web server, the client requests a secure connection to Adobe Media Server over RTMPS:443. Adobe Media Server opens a secured persistent connection to Adobe Connect Media Streaming.

Adobe Captive application provides a graphical user interface to maintain and manage the contents of the game. The process of creating functionalities and applications involves modular action models easy to import, export, and publish. Before implementing the game, a sample preview is generated for simulating the actual final product. In addition, the content could be saved in different formats according to developer choice such as MP4, HTML5, XML, PPT, and so on. With different format output capabilities, end-users could access through mobile, tablet, and PC.

Cybersecurity awareness through fun and gaming should reach all users despite any disabilities. Adobe Captive GUI design offers clear visibility, with audio and video presentations. Hence it complies with Web Content Accessibility Guidelines (WCAG).

IX. APPLICATIONS AND FUTURE FEATURES

Technical and logical security protects and defends attacks originating from external sources. Most infrastructure and personal data breaches occur due to the carelessness and cluelessness of users of the system that originates internally. Education and training insiders and users of any infrastructure helps strengthen the security of any company and ultimately minimizes the number of targeted attacks. Hence implementing web-based cybersecurity awareness games offers a learning experience through fun and entertainment. The platform uses audio, video, quiz, and hints as tools to attract and engage students in securing the organization.

Cybersmart trivia could be implemented to educate users in big institutions, universities, and enterprises for protecting the network and data security of their resources and assets. There are different ways to utilize cyber smart trivia for educational and training purposes. The university could integrate Cybersmart trivia with learning management (Brightspace) and track users' progress periodically. Before issuing the university's login credentials students are encouraged or obliged to complete this training as a way to strengthen the security of the system.

Furthermore, the best way to enhance cyber security training would be to bring students from intra or inter-programs to compete by injecting rewards and/or awards. Competition and gaming offer excellent experiences for students to grasp important messages without putting extra burden on existing courses. External sponsorship or small grants with financial incentives for students or employees participating in competition adds more catalyst to bring about slow and efficient in changing the culture and perception of protecting and securing personal and institutional data.

Some features are important to integrate to maximize the participation and usability. In this game competition format contestants could invite noncontestants for help through voice, video, or chat. University voice-over IP (VoIP) infrastructure could be connected to Cybersmart trivia application through the existing SIP protocol feature of Adobe Connect server. SIP server bridges PSTN telephony and Adobe media gateway through SIP 5060 and RTP 5000-5500 ports. The telephone system and adobe connect communication architecture is shown in the Figure 17 and Figure 18 shows intergartion process specific to our project.Telephone service provides direct interaction between the contestant and the external audience, this serves as knowledge and information sharing. Social interaction and communication expand the awareness of data protection and security [10].

Moreover, voting features could be also integrated by involving competition observants in knowledge sharing with contestants [9]. University information system active directory could be used as a source database list of audiences who are permitted to vote in the system. Linking the Cybersmart trivia application to the existing university database and creating a list of audiences presenting at the venue would be given voting access for specific questions that need voting. Competition between participants should be treated fairly for everyone. The

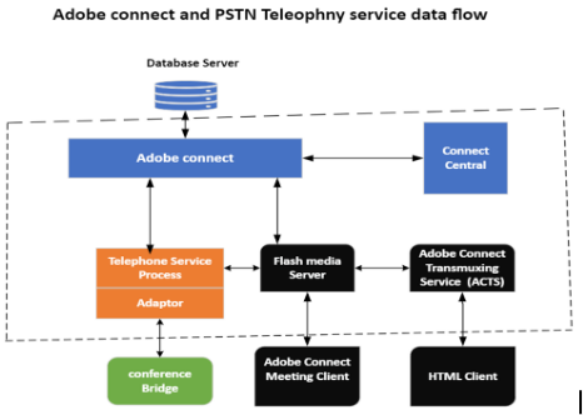

Fig. 17. Adobe Connect and telephone service data exchange flow diagram

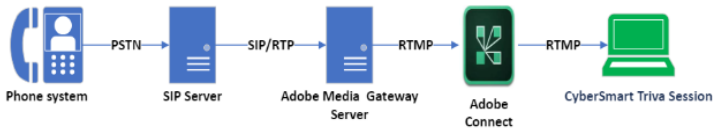

Fig. 18. Summarized workflow for integration of telephone service into CyberSmart Trivia

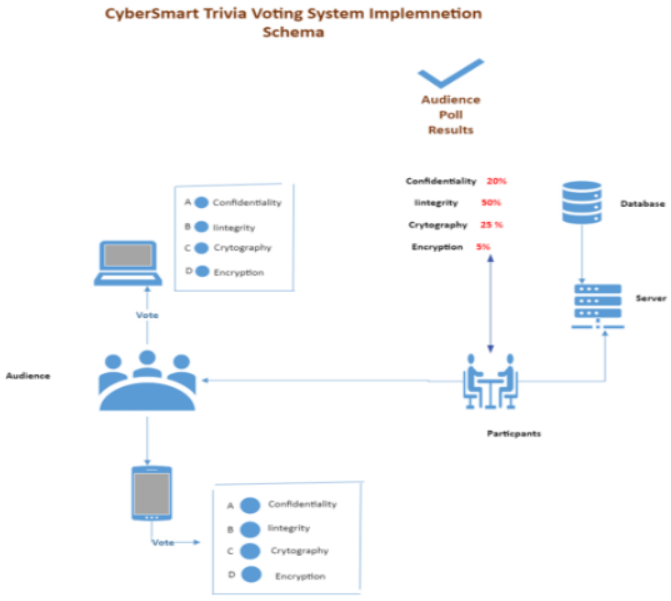

Fig. 19. Voting system implementation schema for Cybersmart Trivia

competition administrator should have the highest privilege to allow for special quizzes where participants invite the audience for voting. Participants would be given the privilege to seek votes for the authorized question. Audience voting results should be integrated into the game application. The vote collected data should be summarized or computed as quantifiable statistics and/or visualization dashboard for assisting the participating in decision making. A schematic implementation diagram is shown in the Figure 19.

X. OUTCOMES OF THE GAME

Our game offers comprehensive coverage of various topics of information security. Attacks like phishing topics like password security have been covered in our game to offer a broader spectrum of questions so that the users can acquire comprehensive knowledge about cybersecurity. The game provides a practical perspective to the players by challenging the players with questions in the form of simulation attack videos. This enhances the awareness of the users aiding them to recognize potential threats and help them to understand how potential attacks are carried out. After the player answers a question, explanatory feedback is provided to the user giving reasoning as to why the correct option is correct and the other ones are incorrect. This feedback helps the users to understand the concept behind a particular cybersecurity incident. This also strengthens the development of decision-making skills of the user.

One of the final outcomes of our game is to report the performance of the employees of a company as Adobe Captivate allows integrating the results with Learning Management Systems (LMS). This feature in Adobe Captivate allows organizations to track employee performance so that the company can identify individuals who require more training in cyber security.

Our game is compliant with WCAG, ie, Web Content Accessibility Guidelines. It is an important aspect of our game as it allows the game to reach a wider audience which includes individuals with disabilities. Compliance with WCAG has been ensured by designing the game to be accessible on various platforms, including mobile devices, following AA conformance requirements, incorporating captions for audio and video content, supporting mobile gestures, providing keyboard accessibility, and taking care of color contrast in the game visuals.

XI. CONCLUSION

The prevention and protection from cyber-attacks include both the use of tools and practical knowledge. The technical solutions provide defense against the external attacks whereas personal data breaches can be prevented by raising awareness of the individuals. Generating awareness about the tools and techniques can ultimately reduce the number of victims of cyber attacks over the course of time. The web-based game developed as a part of this project can play an effective role in providing education regarding cyberattacks and cyber security through entertaining and engaging learning experiences. The

controls and features provided by the game interface provide the means for tracking the user's progress which can help organizations gauge the level of the user and make decisions regarding further training. The gradual increase in the level of the questions makes this game suitable for organizations to provide uniform training to individuals with different levels of skill sets in a particular team.

REFERENCES

[1] J. Espinosa, M.Abellan, A.Moreno et al."Gamification as a Promoting Tool of Motivation for Creating Sustainable Higher Education Institutions." International journal of environmental research and public health vol. 19,5 2599. 23 Feb. 2022 [2] Adobe."Digital Learning Solutions - Adobe Captivate" //www.adobe.com/ca/products/captivate.html (accessed April 19, 2023).

[2] Adobe."Digital Learning Solutions - Adobe Captivate" //www.adobe.com/ca/products/captivate.html (accessed April 19, 2023).

[3] Adobe Captivate System Requirements. (n.d.). //helpx.adobe.com/ca/captivate/system-requirements html.

[4] Wikipedia."Web Content Accessibility Guidelines".https://en.wikipedia.org/wiki/Web Content Accessibility Guidelines (accessed July 10, 2023).

[5] Section508."Applicability and Conformance Requirements for Developers".https://www.section508.gov/develop/applicability-conformance (accessed July 10, 2023).

[6] "Adobe Connect technical overview" [online]: available: https://helpx.adobe.com/adobe-connect/installconfigure/preparing-install-connect.html accessed: between Mar 19- Apr 20, 2023

[7] "Top 10 Web Application Security Risks" [online] available: https://owasp.org/www-project-top-ten/ accessed Apr 5, 2023

[8] "Visio in Microsoft 365 – Diagram and Flowchart Creator" [online] available: https://www.microsoft.com/en-ca/microsoft-365/visio/flowchart-software Accessed: April 10, 2023

[9] "Empower your audience to ask questions, vote in polls interactive quiz for your meeting" [online] Available https://www.slido.com/features-live-polling Accessed: July 7, 2023

[10] "Deploying Universal Voice" [online] available: https://helpx.adobe.com/ca/adobe-connect/installconfigure/deploying-universal-voice.html Accessed: July 1, 2023

[11] "Commix Command Injection Explorer" [online]: Available https://github.com/commixproject/commix Accessed: July 5, 2023

[12] " SIP: Session Initiation Protocol Network Working Group Request for Comments: 3261" [online]: Available https://datatracker.ietf.org/doc/html/rfc3261 Accessed: March 19 - July 10, 2023

[13] "Kali Linux Penetration Testing" [online] available: https://www.kali.org/ Accessed: July 9, 2023

[14] "Apache HTTP Server on Ubuntu" [online] available https://packages.ubuntu.com/search?keywords=apache2 Accessed: July 9, 2023

[15] "Who Wants to Be a Millionaire?" (n.d.). //https://en.wikipedia.org/wiki/Who$_{W}ants_{t}o_{B}e_{a}\,_{M}illionaire$