An Introductory Visualization Aid for Cybersecurity Education

Gabriel Castro Aguayo[1], Ulises Morales[1], Xiaoyu Long[1], Quamar Niyaz[1], Xiaoli Yang[1], Ahmad Y Javaid[2]
[1]ECE Department, College of Engineering and Sciences, Purdue University Northwest, USA
[2]EECS Department, College Of Engineering, The University of Toledo, USA
{gcastroa, umorales, long312, qniyaz, yangx}@pnw.edu, ahmad.javaid@utoledo.edu

Abstract—*As the technology keeps overgrowing, the Internet surfing becomes more popular. As a consequence, users tend to use it for social media, shopping, banking or any other online services in which they need to put their personal information. These online activities attract malicious computer users to apply cyberattack techniques to steal other users information. The users become attack victims due to limited understanding of cyberattacks and safety practices. In this paper, we propose a framework development for interactive and engaging cybersecurity education. With the help of the framework, the users will be able to learn different types of cyberattacks and defenses along with the safe cybersecurity practices. We also discuss the current state of the framework and conclude the paper with discussion on limitations and future work.* [1]

Keywords: cybersecurity education, visualization framework, Unity 3D

1. Introduction

With this technology boom, most people tend to be on their smartphone or computer surfing online nowadays. Even though the Internet makes our lives easy by providing online services such as allowing customers to make purchases online faster than actually going to the stores, some misfortunes can occur when we are using those services. As more people rely on the computers, the more vulnerable they become to any attack. Malicious computer users can find ways to steal credit card or personal information by using malware or backdoor. According to Symantec 2018 report [1], 27% mobile apps in lifestyle category were malicious. That is not the end, the number of new malware variants for smartphones have increased. According to an article in [2], the cyberattack victims lost around $1.5 billion in 2017 and more than 300K Internet crime complaints were reported to the Internet Crime Complaints Center in the same year. The same article mentioned that 23% of Americans in a conducted survey reported that credit card information of their family members were stolen by the hackers.

There are some good practices that one can use to identify these malicious attacks and be properly secured. One good practice is by being observant of any changes on the device or have security software to assist with some automated scan. Another practice is to observe for any unusual activity in a smartphone, such as obsessive data usage or even overheating. Besides, smartphones record events such as installation and data usage that can help narrow down the application responsible for any malicious activities. Practicing cybersecurity methods can help reduce the potential of having information stolen from attackers. However, there is a lack of cybersecurity safety practices among the users. Therefore, it is imperative to spread the cybersecurity awareness through different channels and educate the users how to avoid cyberattacks. Having users practice visually can be beneficial to teach them safe practices of using technology and being online. As cybersecurity visualization can be effective for security analysts to prevent a malicious attack, it can also be helpful to engage users in the learning process of cybersecurity threats and defenses [3].

With this motivation, we propose a visualization-based cybersecurity education framework that will help users, especially the teenagers in middle and high schools, understand the cybersecurity issues they may run into. It will allow them to learn about the attacks that they are exposed to when navigating online, so they can prevent these misfortunes. There are two main reasons to focus on users from early ages. First, they tend to be the future of our society, so they might be the next generation of cybersecurity specialists who might be able to prevent more advanced cyberattacks. Second, the increased usage of smartphones and the Internet by teenagers has brought several security concerns for them and their families. With the increased time spent online, teens frequently encounter cyberbullying or unpleasant experiences. According to a survey conducted by McAfee, 34% teens acknowledged that they have experienced cyberbullying. The same study mentioned that 39% teens do not adequately set their privacy settings [4] for different online applications. The developed framework consists of user-friendly graphical interfaces with different environments to provide cybersecurity knowledge and safety practices to middle and high school students. As the primary target is teenagers for this framework, the development of the personal computer (PC) as well as the tablet/smartphone versions will be available to fulfill every user needs.

The rest of the paper is structured as follows. In Section 2, we briefly discuss the related work. Section 3 discusses the application design of the framework. In Section 4, we discuss various visualization-based cybersecurity education topics implemented at introductory level in the framework. Finally, we conclude our paper in Section 5.

[1]Disclaimer: This work uses popular characters (such as Pikachu) ONLY for educational purposes. There is no intention of copyright infringement. Names, characters, businesses, places, events, locales, and incidents are not our copyright and have been only used to attract young kids towards cybersecurity education. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

2. Related Work

Learning through visualization technologies using computers are mature and widely used in various domains. Learning using tablet/smartphone devices is a relatively new area. There have been studies that involved creating learning applications for smartphone devices, especially for new languages [5]. Apps like Duolingo, Busuu, and many others teach new languages to any smartphone user who installs and uses the apps. Practically anything can be taught nowadays as long as the targeted app is developed for the common user. There are a variety of teaching apps from learning a new language to learn new software. In addition, there are apps that are being used for distance learning [6]. With every student owning at least a computer either PC and/or a smartphone device, any application can be developed to teach the students a subject.

There is a group that created a popular Capture The flag (CTF) game for high school students to learn technical concepts by creating a competitive environment [7]. They introduced it in a GenCyber [8] camp and this motivated the students to continue learning after the camps because of the competition-based game format. With introducing serious game into learning, we bring the concept of visualization and interaction into the design of our framework, as it actively engages users to learn subjects. The learning tool will teach each topic by involving the user in active learning through interactive simulation. In addition, the framework includes assessments to evaluate what the user has learned.

3. Application Design

In order to develop the application framework, various software engines were analyzed, and Unity 3D [9] was found as the best fit. Unity has a variety of tools that offer developers a friendly environment to work on. Although the final design tends to be for smartphone platform, the application will first be built for PC platform to test it prior to the final delivery. Fortunately, Unity allows user to change the platform easily. In addition, the engine provides an integrated development environment (IDE) to write code as well as high visual and audio effects. Therefore, Unity is the best choice to develop the application.

As previously mentioned, the application will be focused on PCs for this design. It will be modified to accommodate smartphone devices upon completion. The application will have a menu, shown in Figure 1, that will help the user to navigate through different topics and be aware of what topic/section they are on. The menu will be made generic so more topics and sub-topics can be added in the simplest way possible. It will have the effect of shrink and expand list to display the sub-topics so that the user is not overwhelmed. Each topic will consist of four stages for the users: i) introduction, ii) interaction, iii) explanation, and iv) assessment. The flow chart can be seen in Figure 2, as to how the flow of the learning module will be for the user for each topic. These tasks are important for the user to understand and evaluate what they are learning.

The **introduction** will be a brief description of what the topic is about; the best way to grab a user's attention is to have an

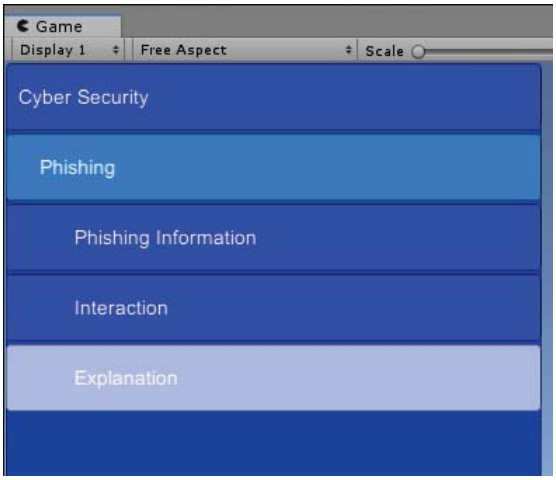

Fig. 1: Menu screen for the topics and sections in the framework

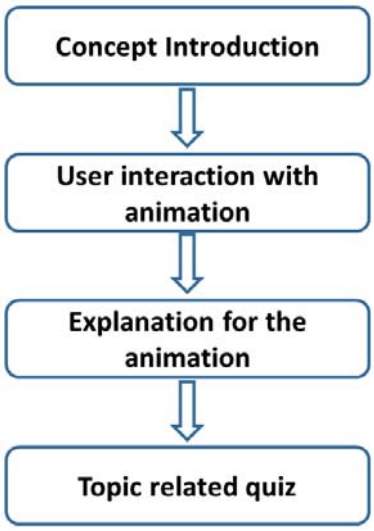

Fig. 2: Stages involved in each learning module

animated character with a short story or description. Even with a little interaction, it is enough to keep the user entertained and learning [10]. The animated introductions will be different for each topic so that the user does not become disinterested with the same animations. The **interaction** is more of a challenge due to the fact that the technical terms and procedures have to be displayed in a way that the user can understand. The display is not the only concern, but the interaction part as well where the user can learn from the stories and get a better understanding of the process and concepts implicitly by interacting with the environment. Moreover, the interactive part should not be long else it will overwhelm the user with more detailed information. With having topics and sub-topics, each interaction will be short and straight to the point, therefore still giving the students the ability to interact and learn the main key points. The **explanation** task will be more in depth where the key points are being explained. This is where the user will get a complete understanding of what they have learned in the interactive task. Just as the introduction, it

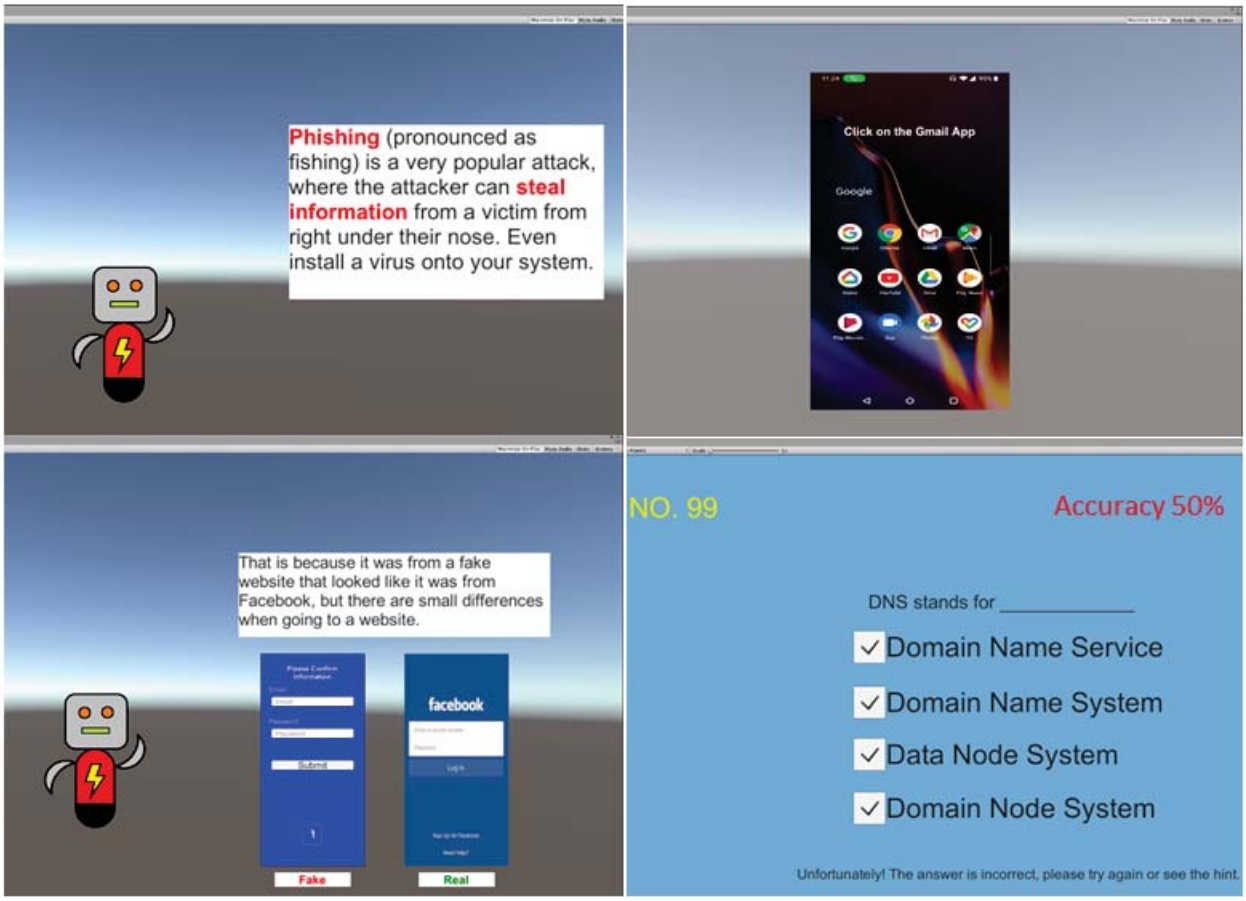

Fig. 3: Learning modules, information (top left), interaction (top right), explanation (bottom left), and assessment (bottom right)

will involve some animation and very minimal interaction in order to have the users complete attention. The explanation will also go over parts that will be reviewed in the quiz. In the **assessment**, completion of the quiz will be recorded in order to know the progress of the user. There will be a set of questions for each topic, however only a few questions will be asked at random so the same questions are not repeated each time. When the progress is recorded there will be a progress bar that will demonstrate how much the user has completed successfully.

Before releasing the final application, testing will be fundamental to assure that the software can be a great tool to acquire the desired cybersecurity knowledge. Testing will be performed to a certain group of students with basic knowledge of cybersecurity who will analyze the application and provide important feedback. Figure 3 shows an example of the four stages of a learning module.

4. Visualization-based Education Topic

There are wide range of topics in cybersecurity. To get started with the framework development, we have considered network and web security. In network security, we have started with TCP and DNS protocols (discussed below) and associated attacks with them. For web security, we focused on cross-site web attacks and phishing.

4.1 Network Security Visualization

4.1.1 DNS Illustration

The Domain Name System (DNS) is used to resolve domain name, e.g. `www.pnw.edu` to an IP address [11]. It is request-response protocol that runs on the application layer of TCP/IP Internet stack. DNS is unanimously used for resolving domain names due to its distributed implementation. For DNS visualization, following questions had been considered:

- What is DNS and how does it work?
- How to make the DNS process easy to explain?
- How to visualize the attacks associated with the DNS?

These questions are answered in the framework. We chose two typical DNS attacks: amplification and hijacking. In the DNS amplification attack, attackers use open DNS servers to flood a victim's network with a large number of DNS reply messages [12]. The attacker sends DNS look-up queries to a large number of open DNS servers by spoofing the IP address of the victim as source. As a consequence, all DNS responses are sent to the victim. In DNS hijacking, the attacker sends the domain resolution query to a different DNS server instead of the actual ones.

For the introduction stage of DNS module visualization, a daily situation has been taken for illustration. How would you

Fig. 4: Introduction and interaction stages for DNS module

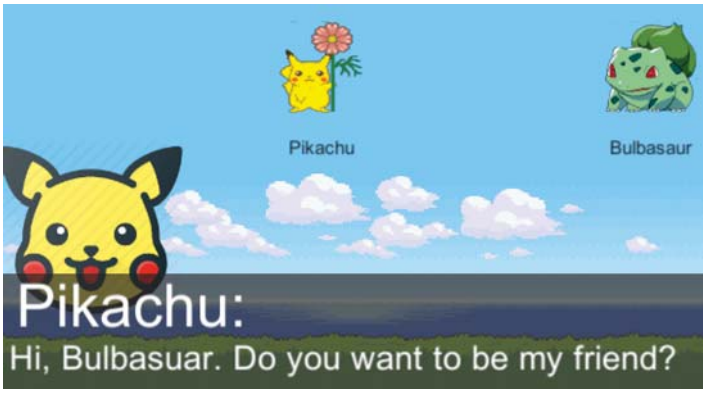

Fig. 5: Game-based visualization to explain TCP connection set-up

find the location of a new address? A man called Bob has to find the address for Google's office "1600 Amphitheatre Pkwy, Mountain View, CA 94043" (in an age with no Google Maps). To visit Google, he goes to the local community office to obtain knowledge of the new address; the local community office represents the local server. The local community office gives a part of the address to Bob such as that the Google's office is in California state. Then, Bob goes to California and asks the state government staffs, city staffs, and Google's neighborhood as shown in Figure 4. These represent root server, TLD (Top Level Domain) server and domain nameserver, respectively. In the DNS amplification attack, the interaction is based on the DNS concept and developed on top of it. In DNS hijacking interaction, it shows that a dishonest staff will provide wrong information. According to the interaction, users can easily understand the DNS process and how attacks may happen through DNS.

4.1.2 TCP Illustration

Transmission Control Protocol (TCP) provides reliable communication between two hosts that is achieved by a "three-way handshake" [13]. There are three steps in this handshake process. First, the client sends a connection request to the server using some initial sequence number, and a window size for the buffer used by the client to store the packets coming from the server. After receiving the request, the server sends a message to the client including its randomly chosen sequence number and window size along with the confirmation of client's sequence number. After receiving the response form the server, the client returns an acknowledgement message with the confirmation of server's sequence number and then a TCP connection is established.

To make this process more understandable, we made a dialog-game how two cartoon characters make friends shown in Figure 5. In this game-based visualization, Pikachu represents the client and Bulbasaur represents the server. In the beginning, Pikachu will send a friend request (first step). Then, Bulbasaur replies to the request and sends the friend acceptance (second step). After Pikachu confirms the acceptance (third), the friendship between Pikachu and Bulbasaur will be established. We have also added a learning module for TCP SYN Flooding attack.

4.2 Web Security Visualization

4.2.1 CSRF Attack

CSRF stands for cross-site request forgery. In this attack, an attacker creates a forge request for a trusted website. The request appears genuine to the trusted website [14]. One purpose for CSRF attack could be modify information in social media or banking system.

As many users are familiar with the social media, CSRF visualization shows the social media website of two users (Sammy and Alice), example adopted from SEED labs [15]. Sammy is trying to become friend with Alice, but she does not accept his friend request. Then, Sammy uses CSRF to generate a request from Alice' web browser using which she logged-in to the social media server. Sammy create a forge request and embeds it an external website. He sends the link to Alice to open it. Alice, then, get affected by the request. The user will be able to interact with both the characters in order to learn the functionality of CSRF, shown in Figure 6. At the same time, definitions and explanations will be shown. A quiz after every level will be pop up to measure whether the user understood the topic or not. Furthermore, the user will also be able to see how the process of CSRF works in an abstract way.

4.2.2 XSS Attack

XSS attack stands for cross-site scripting attack. It is an injection attack that affects web application with vulnerabilities. Attackers can manipulate and inject malicious code in web pages. Once the user accesses the web page, the malicious code executes in his/her system [16].

As mentioned in CSRF visualization, social media is popular among the Internet users around the world. XSS visualization will also show how XSS can be injected in a social media website. For this case, Sammy will inject malicious code under his profile with JavaScript language. So every user who visits Sammy's profile, his/her profile will be updated due to the malicious code [17].

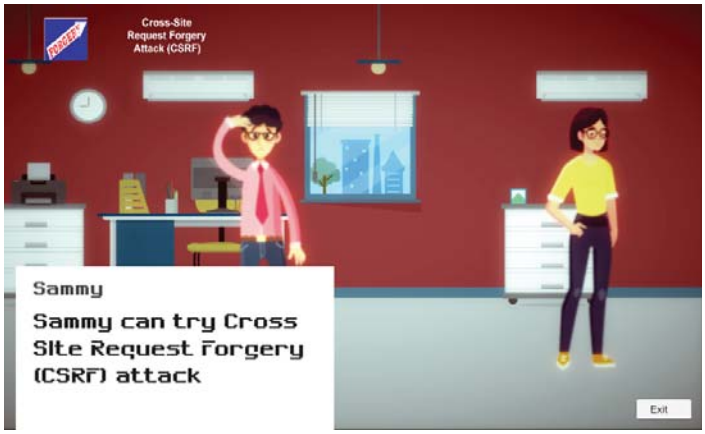

Fig. 6: GUI of CSRF attack visualization

4.2.3 Phishing Attack

It is an attack where the user provides information to an attacker unknowingly. The common way this occurs is for the attacker to create an email while imitating to be a known third party, such as a bank or social media customer service [18]. When the user clicks on a link or download an attachment, one of the two things can happen; one, the link will guide the user to a fake website imitating a legitimate log-in to get account information or even credit card information; or two, the downloaded attachment may contain an infection and installing a malware on the user's computer/mobile device.

The design of the interaction part will assist the user to understand what a sample phishing email will look like and how to avoid it shown in Figure 7. A typical phishing attack may not seem as an attack at first, but as a genuine email from a third party. In the interactive part of this attack, the user will be using a mail app to open their incoming email. Within the incoming mails, there is an email from Facebook pretending to be from customer service; when the user goes to the link that the email provided it will redirect the to Facebook's log-in page. The user will put in their log-in information, however once the user enters it and attempt to sign-in a warning will pop-up notifying the user their information has been stolen. This occurs in everyday life where people's information gets stolen without warning.

5. Conclusion and Future Work

As the usage of the Internet keeps growing, users need to understand the risk they are exposed to when navigating to websites. The main objective of our project is to spread awareness of cybersecurity and educate the users how to detect and avoid cyber attacks at a young age. The framework will not only allow the users to learn the different kinds of attacks that adversaries may use, but the ways they can defend from them.

Currently, we have implemented a few security examples in the application. We understand that the framework has several limitations, primarily in terms of content and student assessments. In future, we plan to include more attacks and defense mechanisms in the framework. As this framework application will first

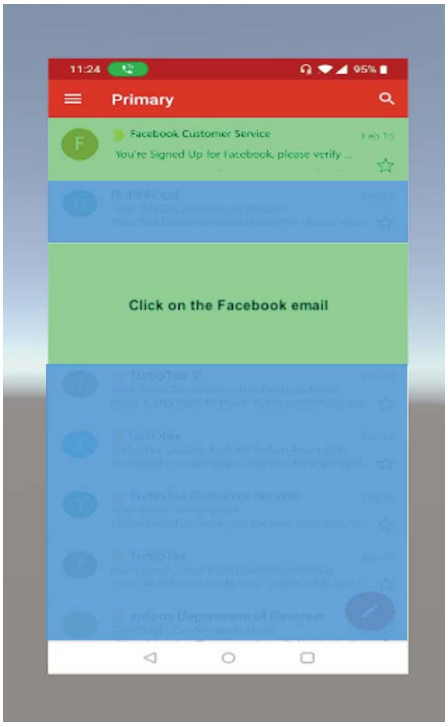

Fig. 7: Phishing Email Visualization

be built and tested for PC platform, another future work would involve creating a mobile-compatible version. We plan to use this framework for delivery of a cybersecurity basics course, assess the effects of this framework on learning and prepare a continuous improvement plan (CIP). This CIP would include improving specific modules that can enhance users' understanding, based on the user assessment. In order to keep the user engaged in a game-based learning environment, more levels will be developed where the progress and scores will be visible to the users. Finally, we plan to make this framework open source to the academic community after development and assessment.

References

[1] "10 Cyber Security Facts and Statistics for 2018." https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html Accessed May 15, 2019.

[2] A. Zangre, "50 Noteworthy Cybercrime Statistics in 2019." https://learn.g2crowd.com/cybercrime-statistics Accessed May 17, 2019.

[3] D. Schweitzer and W. Brown, "Using visualization to teach security," *J. Comput. Sci. Coll.*, vol. 24, pp. 143–150, May 2009.

[4] "Cyberbullying Triples According to New Survey of Teens Online." https://homeword.com/2014/06/10/cyberbullying-triples-according-to-new-survey-of-teens-online Accessed May 15, 2019.

[5] R. Godwin-Jones, "Mobile apps for language learning," *Language Learning & Technology*, vol. 15, no. 2, pp. 2–11, 2011.

[6] E. Vázquez-Cano, "Mobile distance learning with smartphones and apps in higher education.," *Educational Sciences: Theory and Practice*, vol. 14, no. 4, pp. 1505–1520, 2014.

[7] L. McDaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5479–5486, IEEE, 2016.

[8] "GenCyber." https://www.gen-cyber.com/ Accessed May 17, 2019.
[9] "Unity." https://unity.com/ Accessed May 15, 2019.
[10] L. Blasco-Arcas, I. Buil, B. Hernández-Ortega, and F. J. Sese, "Using clickers in class. the role of interactivity, active collaborative learning and engagement in learning performance," *Computers & Education*, vol. 62, pp. 102–110, 2013.
[11] "DNS." https://en.wikipedia.org/wiki/Domain_Name_System Accessed May 15, 2019.
[12] "DNS Amplification Attacks." https://www.us-cert.gov/ncas/alerts/TA13-088A Accessed May 15, 2019.
[13] "TCP." https://en.wikipedia.org/wiki/Transmission_Control_Protocol Accessed May 15, 2019.
[14] "CSRF." https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF) Accessed May 15, 2019.
[15] "SEED Labs." www.cis.syr.edu/~wedu/seed/labs.html Accessed May 15, 2019.
[16] "XSS." https://www.vpnmentor.com/blog/top-10-common-web-attacks/ Accessed May 15, 2019.
[17] "Sammy Worm." https://en.wikipedia.org/wiki/Samy_(computer_worm) Accessed May 15, 2019.
[18] "6 Common Phishing Attacks and How to Protect Against Them." https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/ Accessed May 15, 2019.