8-2022

Securing Information on a Web Application System to Facilitate Online Blood Donation Booking

Hrishitva Patel
University of South Carolina - Columbia, hpatel51@binghamton.edu

Publication Info
Preprint version 2022.

Securing information on a web Application System to Facilitate Online Blood Donation Booking

Abstract

Blood donation has saved many lives in the past. According to the American Red Cross statistics, a patient needs a blood transfusion every two seconds. Many benefits arise from blood donation to both the donor and the blood recipients. With blood donation, cancer patients, people involved in accidents, or those battling diseases that require blood donation have access to enough blood to sustain their survival. There is a need to digitize the blood donation booking to facilitate blood donation across the United States, and ensure patients in need of blood, receive their donation from eligible donors on time. This report demonstrates the security measures implemented to secure patient and blood donor data on a blood donation booking web application.

Introduction

Blood drives in regions like sub-Sahara Africa have previously been forced to displace blood from donors after it was found not eligible for donation to recipients. As much as blood donation improves the personal health of the donors by reducing blood pressure and chances leading to heart attacks, several valid reasons disqualify donors from the donation. [1] These include age, sexually transmitted disease infection, last blood donation date, and weight.

Blood donors are expected to be healthy and free from blood-transmitted infections like hepatitis, AIDS, and other sexually transmitted diseases. A donor cannot donate more than once in 16 weeks for men and 18 for women. People with tongue piercings, belly button, nose, or genital piercings are not allowed to donate blood if the piercing occurs within a year. People suffering from high or low blood pressure are disqualified from donating blood. Those who weigh less than 110 pounds or are under the age of 17 years are not allowed to vote.

Since the beginning of the AIDS pandemic declared in the 1970s, the United States government disqualified blood donation for men proven to engage in the same sexual activities as a group due to the increased risk of HIV, and hepatitis B, among other infections that arise from a blood transfusion. Hospitals may lack the foundations to check for these criteria and use them to qualify and disqualify donors before they could donate and let their blood go to waste as it's not eligible for use by the patients[3]. A web application is developed to anonymously allow users to check

their eligibility status before they can book for the blood donation process. Information is stored securely in a database on an uploaded server. This facilitates ease of access to the requested information over authorized users.

Blood is donated for different reasons in hospitals and other blood banks. It is essential to help blood recipients survive surgeries, cancer treatment, and chronic illnesses, among other illnesses. The World Health Organization describes blood as the most precious gift a person can give to a person in need of it. Blood donated comprises four components: platelets, plasma, white blood cells, and red blood cells. Cancer patients require a blood transfusion to enhance platelets back into the body after radiation therapy. With a developed web application to book a blood donation session, it is easier for hospitals to know which blood component they need most and thus inform the system administrator to prompt for more blood donors.

Blood donors currently receive notifications about blood drives and donations with the support of social media platforms or other conventional media such as television or newspapers. They lack a dedicated web application platform that avails donors of information about blood drives or blood donor records[2]. It's tedious for hospitals to access information about blood donors, especially in events in which the donors have donated blood more than once without the support of a centralized database. Each blood bank relies on its database or file to access information on donors. This can be quite tedious, especially when there is a blood type shortage and urgent access to a specific blood type is high.

Project Objectives

To address major problems related to blood donation booking for hospitals around the United States, a web and mobile application is developed to ensure;

1. An online platform can notify blood donors of their eligibility to donate blood based on the qualifying factors.
2. An online web application that supports eligible blood donors to book appointments on their most convenient blood drives and dates.
3. A friendly application allows users to securely send privileged information to a credited administrator and receive feedback based on their queries.
4. A remarkable system allows users to watch video testimonies from patients who have benefited or recovered through the help of blood donations.

5. An application allows hospitals to alert the administrator when a certain blood type quantity is low in their blood banks.
6. An app allows users to input and store their user information and send it to the administrator panel.

Project Scope

The web application is developed to process user eligibility before they are allowed to book a blood donation. Records from user input are stored remotely on a database server. There are two types of users for this web application: the blood donors and the system administrators who determine user eligibility based on selected criteria. The system administrators then send the hospital and the eligible donors a date for them to reserve a blood donation.

The user has no system privileges, and they can only register and log in to create a user session that allows them to upload video testimonies and view video testimonies from other donors. They can input their information forwarded to the administrator panel with the system privileges to perform all CRUD operations within the scope of the web application.

The records from user information include the user email, user password, user contacts, user videos, and user messages. The administrator panel consists of the following: managing user information, hospital information, managing videos, and managing messages. Other data include the play store download link for the mobile android application.

Information security techniques have been applied on all web pages to ensure only authorized system users can access the web and mobile applications. With the application operating overactive internet connections, the vulnerabilities that would, in turn, expose the application, data, and the entire network to cyber attackers are patched securely.

System Design

User Page

The blood donors must create an account before they log in and can access a system session and the application's resources. The user form input fields are validated to ensure that only the user's required data types are keyed in. Registration and login information keyed in by the user is sanitized through the POST method to ensure that the database contents are not revealed over the URL bar, thus reducing the chance of interception by an attacker[4].

Credentials such as passwords required to access the system resources are encrypted to ensure a man-in-the-middle attack does not occur between the information sent or fetched from the connected database server.

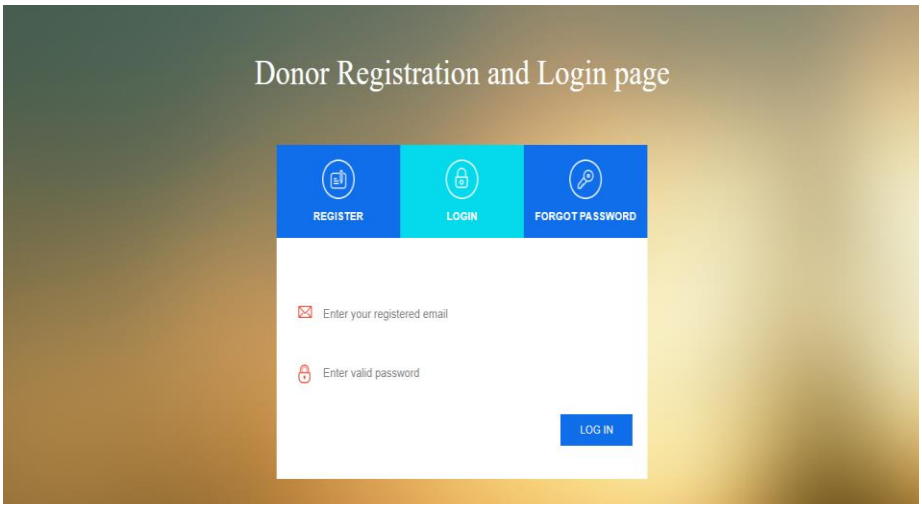

Figure 1: Login and Registration user input

The home page is only accessed once a registered user inputs correct credentials that match those on the database server. Session cookies are disabled on the home page to prevent a cross-site scripting attack. The link to the mobile application is linked to the home page to ensure that users only get the app from trusted sources.

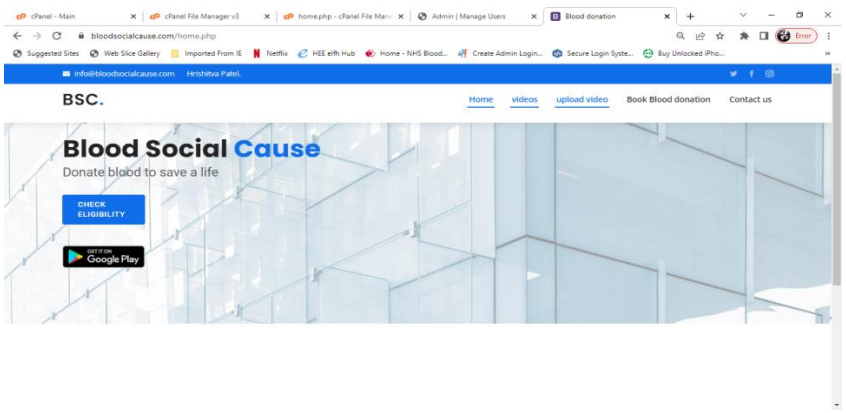

Figure 2: Home page

The developed homepage contains some factual information about blood donation that emphasizes the need to donate blood to maximize saving lives in the United States and the rest of the world. The data displayed on the home page footer is referenced from nonprofit organizations like the Red Cross foundation.

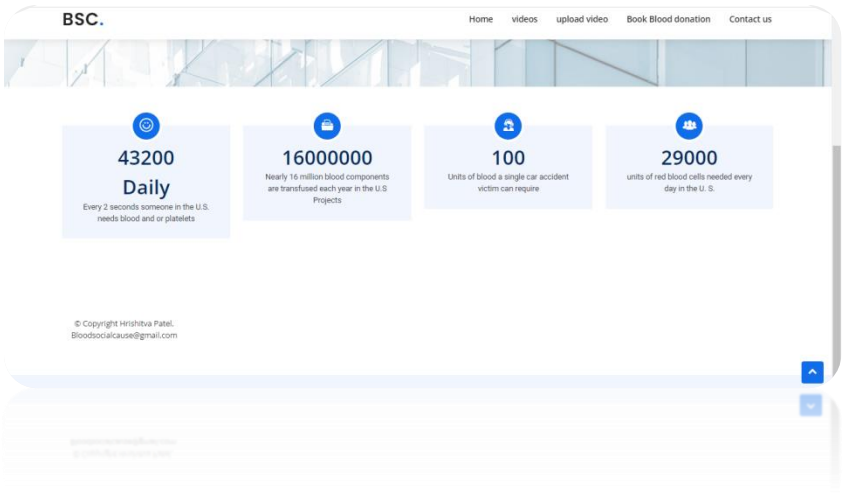

Figure 3:javascript blood-related facts

The uploaded videos are viewed on the video page. The users can only upload a video, while the administrator can delete a video from the server to ensure only authorized videos are added to the web application.

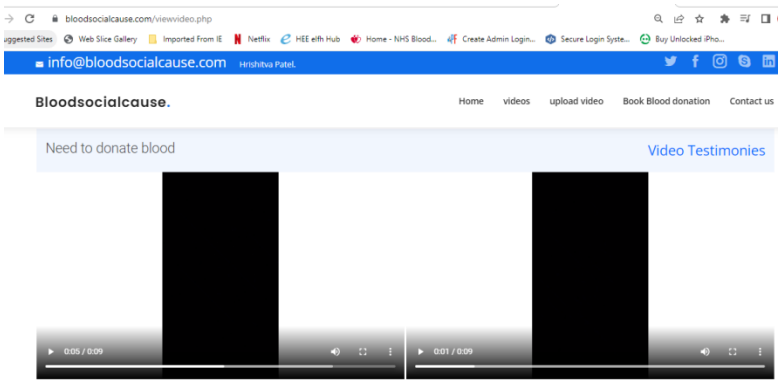

Figure 4: Video page

The video upload page is developed to ensure that only the validated content is uploaded to the server. The administrator inspects cross-site scripting content attached to media stored on the application once a video upload is made. Any media intercepted with an attack script to give unauthorized users access to the system is removed before an attack occurs.

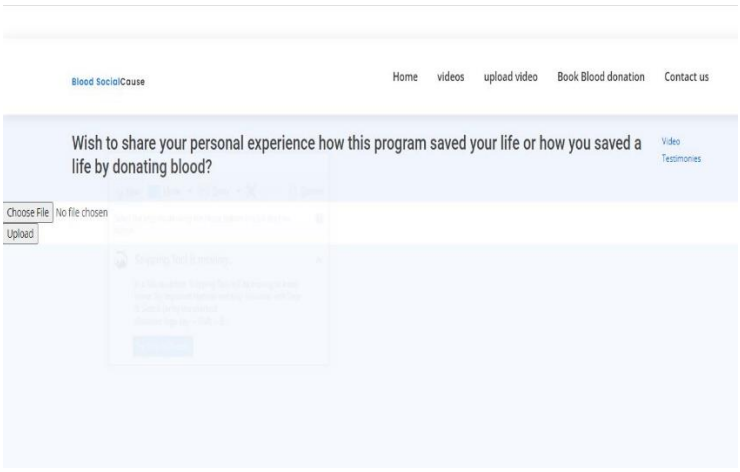

Figure 5: Video upload page

The contact us PagePage is validated to ensure that only authorized data types are keyed into the users. The page is scripted in PHP, and the data is sanitized to ensure that the application is not exposed to attackers.

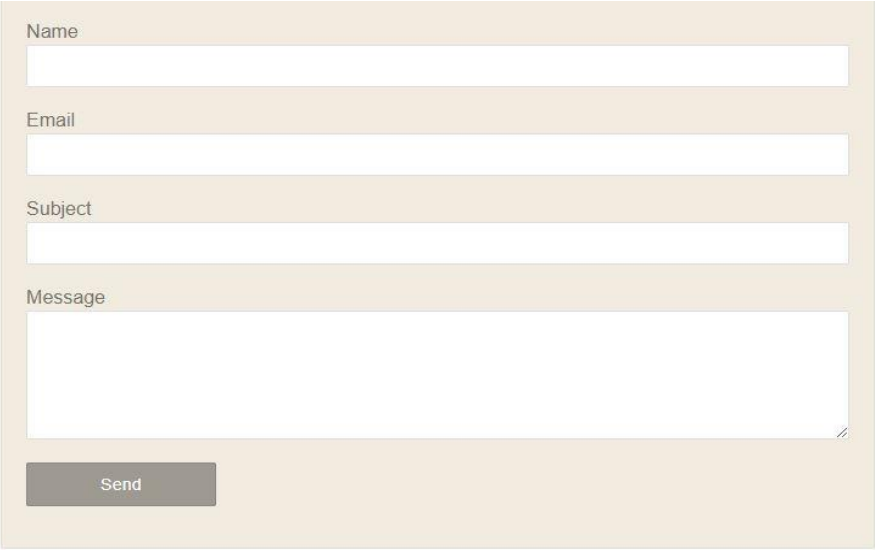

Figure 6: Contact us Page

Admin Panel

The admin dashboard contains all the CRUD functionalities limited to the donors. The administrator's interaction with the system is limited to checking buttons that command function once the user clicks on them. Reducing form input reduces the chance of a malicious code injection being used to exploit the connected instance.

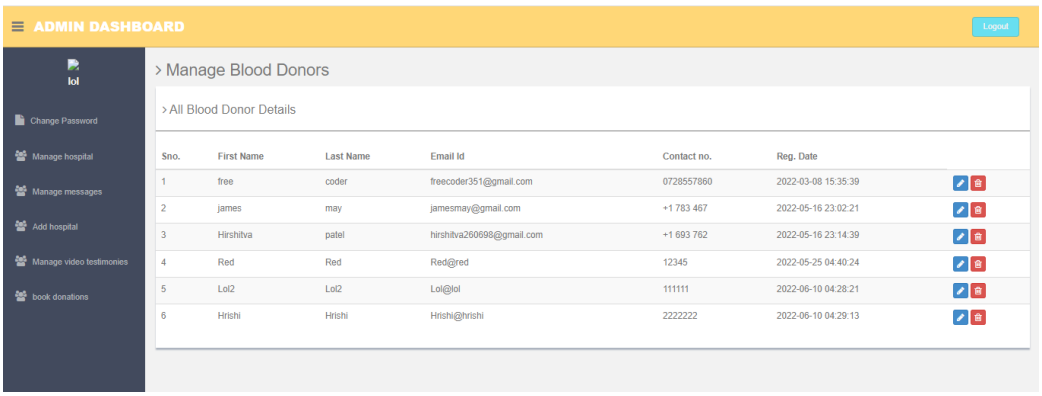

Figure 7: Manage donors' page

The hospital panel is included, too; the administrator has the system rights to add or remove hospitals from the web application.

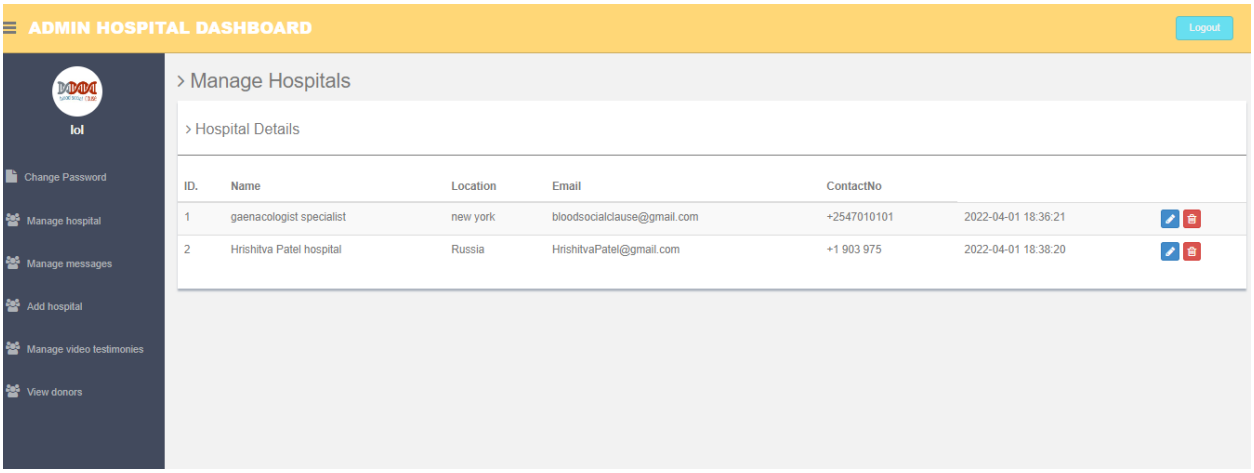

Figure 8: Manage hospital information

Donor and system users' messages are uploaded on the same page to give the administrator a centralized view of all messages sent to the admin.

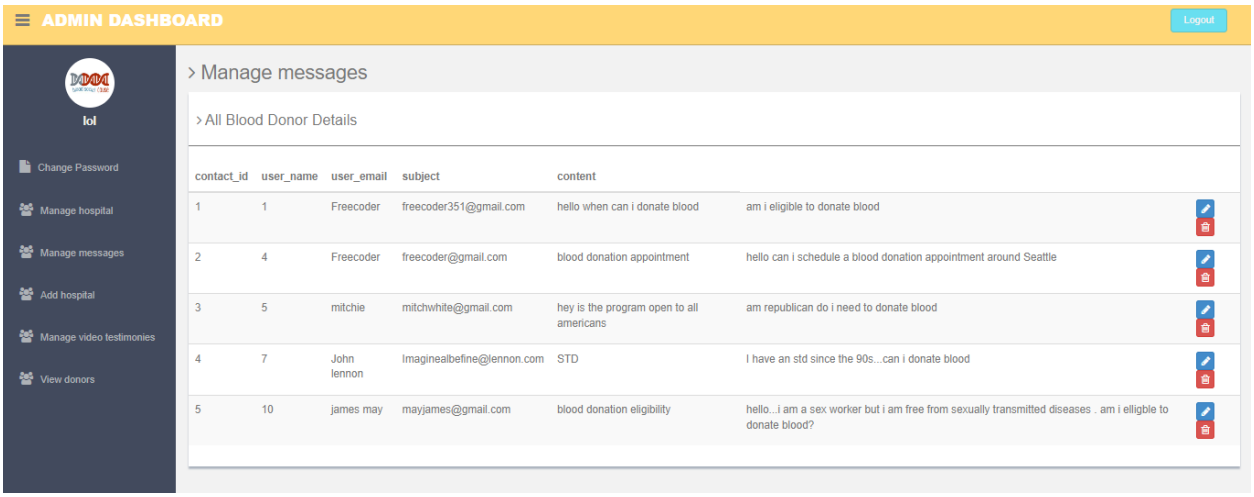

Figure 9: Manage messages

The administrator holds the right to add new hospitals to the web application.

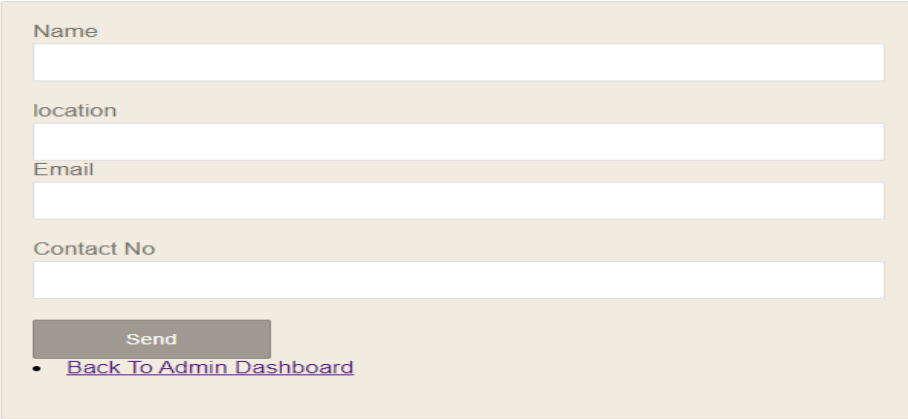

Figure 10: Add hospitals

The administrator has the right to download videos and delete them if an anomaly is detected within these clips uploaded by users. XSS-led attacks are present in media intercepted with malicious code, which cyber attackers exploit to gain access to the web application.

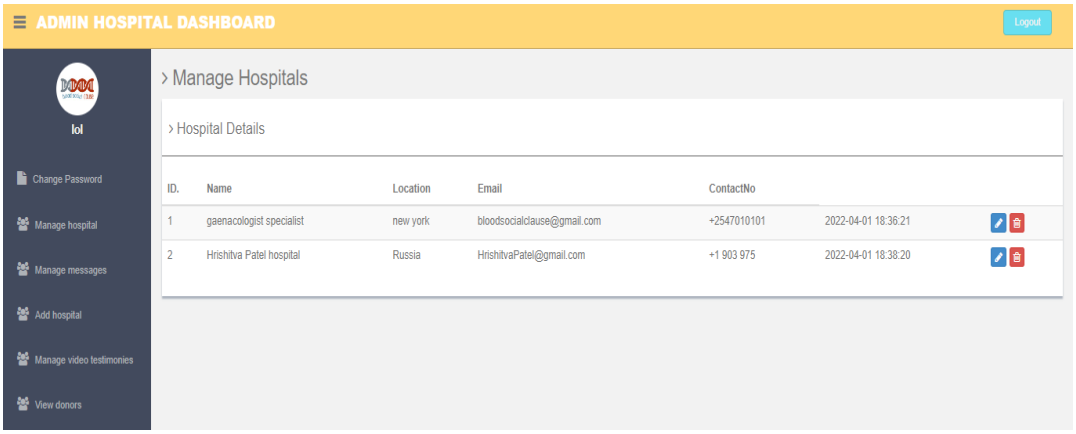

Figure 11: manage video testimonies

Backend Database Security

Database security for the application is met through encryption for the credentials that users require to gain access to the web application. Encrypting privileged information ensures that data transmitted from the user input forms and the database servers are secured from exploit attacks such as man-in-the-middle attacks and other phishing attacks by cyber attackers.

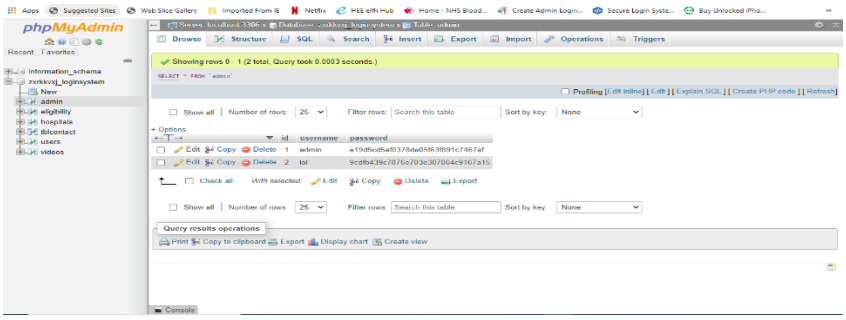

Figure 12: Encrypted login credentials on admin panel

A burp suite analysis was made on the user's page. For this penetration test, the developer decided to decrypt the user's password credentials to show comparison and contrast between 2; the admin and user databases.

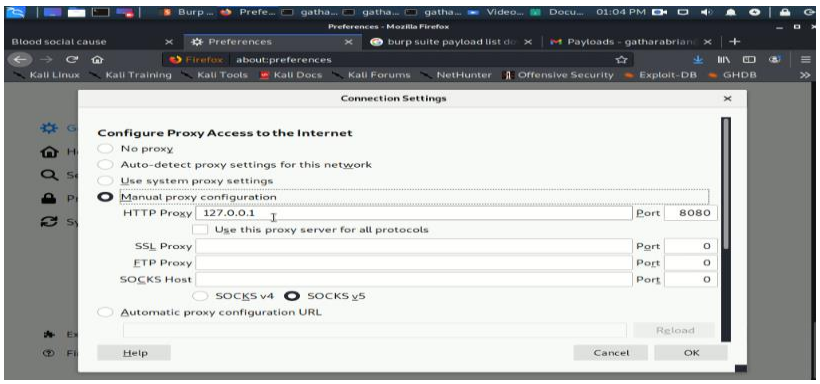

Figure 13: Proxy configuration

The home page on the user page is intercepted using the burp suite. This allows the burp suite to intercept all the web pages and the traffic that the web page transmits.

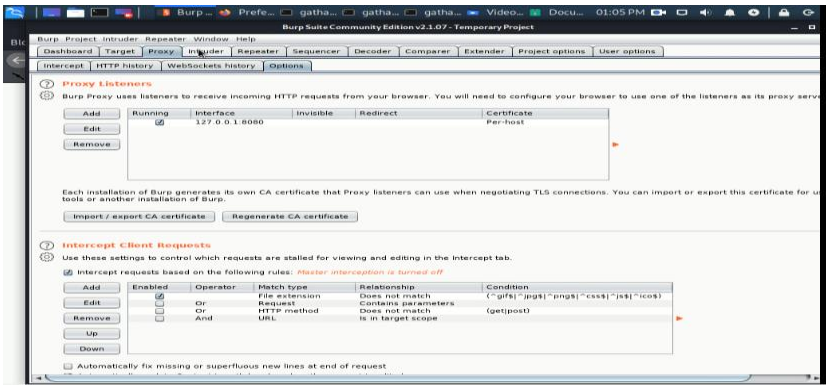

Figure 14: intercept and intruder

Once the website has been intercepted, the payload from figure 14 is loaded on the input forms, and an attack is launched on the targeted web application.

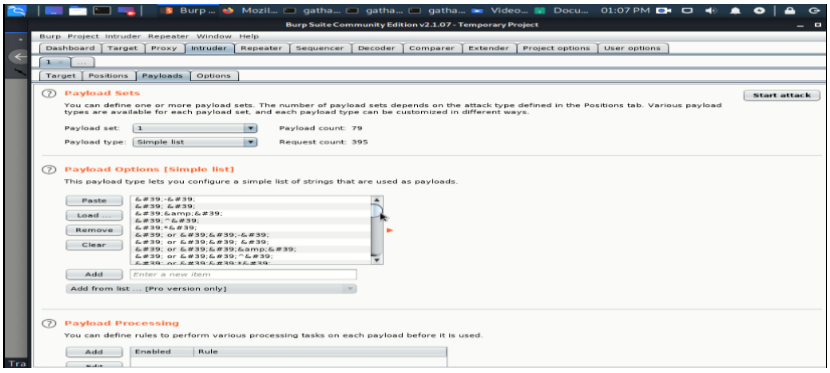

Figure 15: Target intercepted

The payloads include SQL statements that inject code into the database to try to match or bypass login credentials. This is done by the repeater tool on the burp suite.

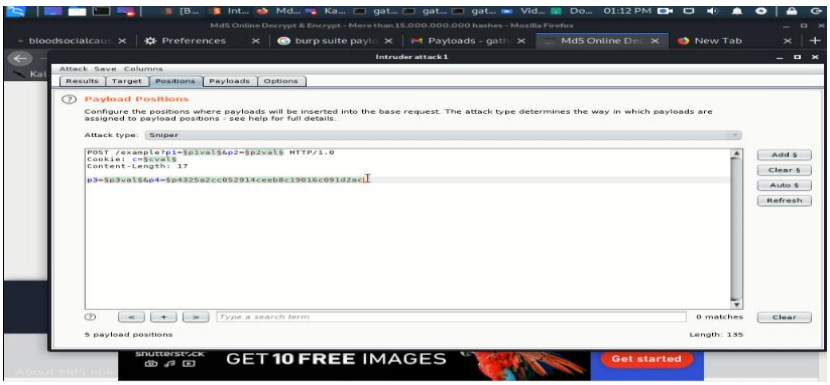

Figure 16: burp suite encrypted digest

The results of the repeater are encrypted as a message digest. The decoder decrypts the message digest, and the password is derived. The burp suite scan doesn't work on the intercepted admin page as the credentials are encrypted.

Open Ports Scan by Nmap

Network mapper (Nmap) is a toolkit that functions to implement networks and perform penetration testing through port scanning and vulnerability analysis. This toolkit works through Nmap scripting engines such as Vulcan, vuln, and vultures which are all categorized differently per function. The functions supported by Nmap scripts are authentication, broadcast, brute force, and malware detection, among others.

Reconnaissance being the first phase of penetration testing, hackers exploit Nmap to locate flaws and loopholes in a targeted system before an exploit attack is launched. Nmap works by transmitting data packets to the target application and, in turn, receiving the responses from the sent packets[5]. This can work over remote connections over different network connections. Web and mobile application servers rely on incident detection systems and firewalls to allow system analysts to detect Nmap scans on their web systems.

AnotherNmap command is run on a kali Linux terminal on the target web application. The results are shown in the figure. The server's credentials were exposed from the open ports while the closed port kept the web application secure.

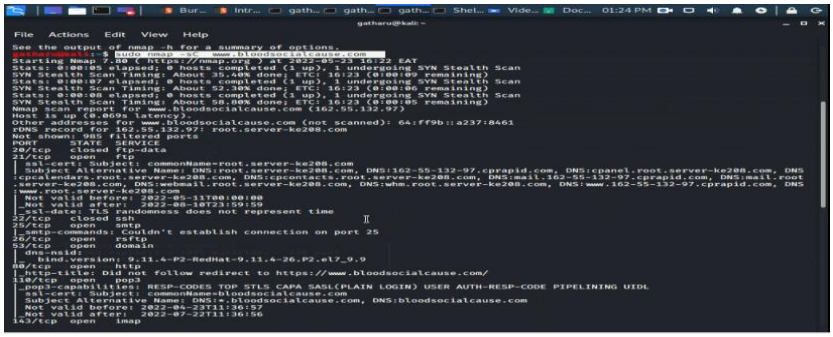

Figure 17: Nmap scan

Distributed Denial of Service Attacks through Nmap

Threat actors can integrate decoys or forge host IP addresses before conducting a port scan on a target device network. This makes it easy for the packet transmission to go undetected over intrusion detection systems implemented on the target network. Distributed Denial of services attack is launched over Nmap through the open ports that cause the network topology supporting the web application to be vulnerable to topology attacks like DDoS[8]. A topology-led attack on a web or mobile application functions triggers many commands and instructions the server cannot accommodate, thus overwhelming it from allowing further instructions from users. The attackers then exploit this opportunity to bypass security bounds on the application and access the application and its hosted resources.

Attackers use Nmap as a tool to run a denial of service attack. This is by running the following script command on the Nmap terminal on the kali Linux terminal; Nmap -v --script dos www.bloodsocialcause.com.

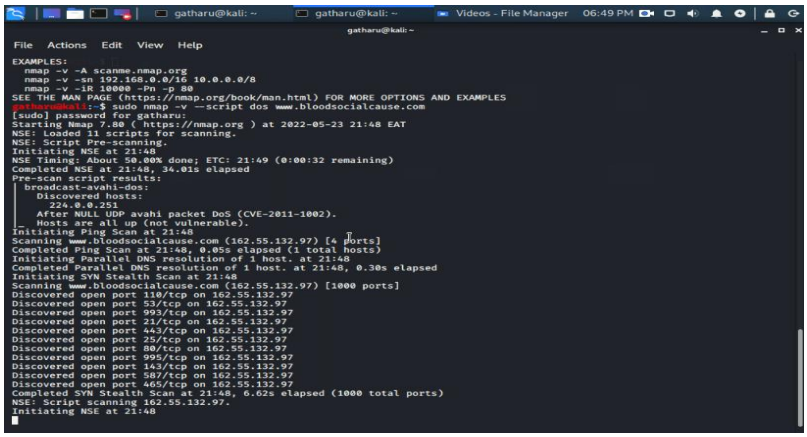

Figure 18:DDoS attack launched over Nmap script

From Figure 18 above, a Nmap DDoS script is launched on the target web application; bloodsocialcause, the script analyzes the whole network, and from 1000 ports, around seven open ports are discovered. These leave the server vulnerable to the incoming distributed intrusion commands on its server, making it overwhelmed to even load the application on the hosted domain.

Reverse Shell Exploit

A reverse shell exploit allows hackers to successfully target web application systems by exploiting the application's control signature. Once the signature is compromised, the application recognizes the attacker's signature as authentic, thus giving them root shell access to access user information on the hosted system[6]. Malicious payloads are executed on the on-host application, which counters or bypasses the defense security certificates over internet gateways. This allows the attacker to gain access to the targeted web application and allows them to write and execute code unauthorized.

The goal of an attacker when running reverse shell attacks is to initiate a shell session from the present web application and launch a shell session. The attacker uses a remote computer as the host to target open ports and vulnerable frameworks on the victim application. From this remote connection, the attacker can establish device communication or take control of the system to manipulate data as they please.

On the Metasploit framework terminal, a backdoor channel is set on the set target web application. An attacker uses the KaliLinux terminal editor to gain root access to the web application through a backdoor channel. The exploit allows the attacker to view the users' database, but from the security patches implemented, a session is not created to give the attacker root access.

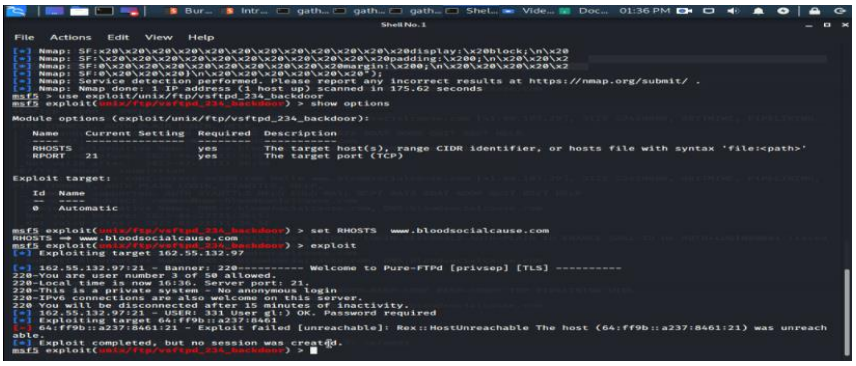

Figure 19: Reverse Shell exploit

They lack a defined single approach or technique to be considered against malicious payloads and code to secure targeted web applications against reverse shell exploit. There are genuine uses to performing a reverse shell penetration test on a web application server system, but with the rise in cybercrime, the technique is used by attackers to launch operating system commands. To fully protect the targeted web application from reverse shell attacks, the developer team should set up proxy servers that minimize the attack surface by restricting packet destination and controls.

Minimizing the number of interpreters will restrict the execution of reverse shell code, making it harder for attackers to exploit the server system [7]. This method may not be viable, especially in the event an attacker works with a shell script that works on hardened servers. Running penetration test assessments to reduce the number of vulnerabilities present in a framework may allow a developer to regularly set up patch updates to affect information security on developed web application frameworks.

On-premise system attack with Rubber Ducky

Cyber-attacks on targeted web and mobile applications are common over remote connections, but this doesn't leave out the fact that on-premise cyber-attacks do not occur over web applications and connected systems. As reported by IBM, insider threats in organizations account for more than 40 % of the total cyber-attack incidents in organizations. Insider attacks are fueled by malicious rogue employees or unknowing employees who are used as attack vectors by the attack's perpetrators.

A common way to launch an on-premise attack is through intercepted universal serial bus drives, commonly referred to as a bad USB or rubber ducky attack. The USB rubber ducky resembles a normal USB drive. Still, it's preinstalled with malicious software to allow cyber attackers to access a victim's device through the remote controller saved on the USB drive memory.

A payload is scripted for a rubber ducky and may be device specific to only work on a particular computer component like a keyboard or an optical scanner. The attackers must perform a background search of the device they wish to target to ensure the bad USB is coded to exploit it(Prasad, 2018). The attackers are then required to pick their target computer device and write code that goes hand in hand with the device properties. Once the payload has been written, it is

deployed on the targeted device. Physical access to the targeted system is required to allow the payload is injected into the targeted device.

```
REM A one-liner to add user "lol2" (password "lol") to the admin group and share the https://www.bloodsocialcause.com/admin

DELAY 1000

GUI r DELAY 100

STRING powershell -Exec Bypass "saps cmd '/C net User ts ts /ADD&net LocalGroup Administrators ts /ADD&netsh advfirewall firewall set rule group=""""File and Printer Sharing""""  new enable=Yes&net share ts=c:\ /UNLIMITED&icacls c:* /grant ts:(OI)(CI)F' -Verb RunAs"

ENTER

DELAY 1000

ALT y
```

The above ducky code instructs the target device system to bypass the admin page for the web application login input credentials. The payload saves itself in location C of the device computer after ten seconds of system access, and it's automated to always check the password for user admin lol every time they access the admin page.

Rubber ducky is highly detectable to organizations that support intrusion detection systems and firewalls in their network. Organizations implement policies to restrict users and employees from bringing their devices to work to reduce the risk of attack or exposure from many devices(Prasad, 2018). Some policies ensure that devices connected to the web and mobile applications boot from a specific network address and that their USB ports are locked for users who lack high privileged mandatory access controls over the targeted system.

Organizations that implement a policy that allows their employees to insert USB drives in their systems may choose to provide them with the USB themselves, and they should ensure that the USB drives are branded and from certified technology manufacturing companies. This would, in turn, minimize the risk of system attack through rubber ducky USB drives.

Mobile Application Server Security

Google play's services affect information security on their play store in various ways for its users and developers. While uploading an application on a google play account, developers are expected to upload a signed android application bundle file that is registered with an encrypted key. For any update that relates to the draft or published app, the developer is expected to sign new updates with the same key, or this would result in an error. This ensures that in the event cyber attackers compromise the google play account, they would still require the key for them to make an update or change the published app.

Figure 20 shows the error that the google play account prompts to the developer in the event they upload an app file whose signed key doesn't match with the published application or the uploaded draft.

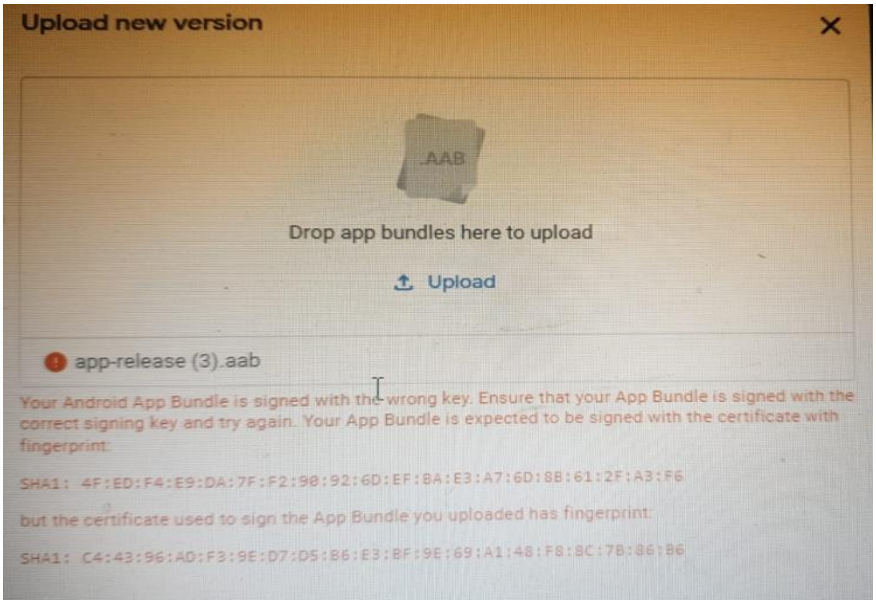

Figure 20: Error result from an aab file signed with two different keys

Google application developers are expected to develop applications that are free from malware or other viruses that may harm android users' devices and compromise their information to cyber attackers. This google play protection gives users full disclosure Onan app that functions by collecting user data, warns them of malware present in an app, file and information sharing, and ensures that the users of the mobile application download are from trusted sources over secure internet connections.

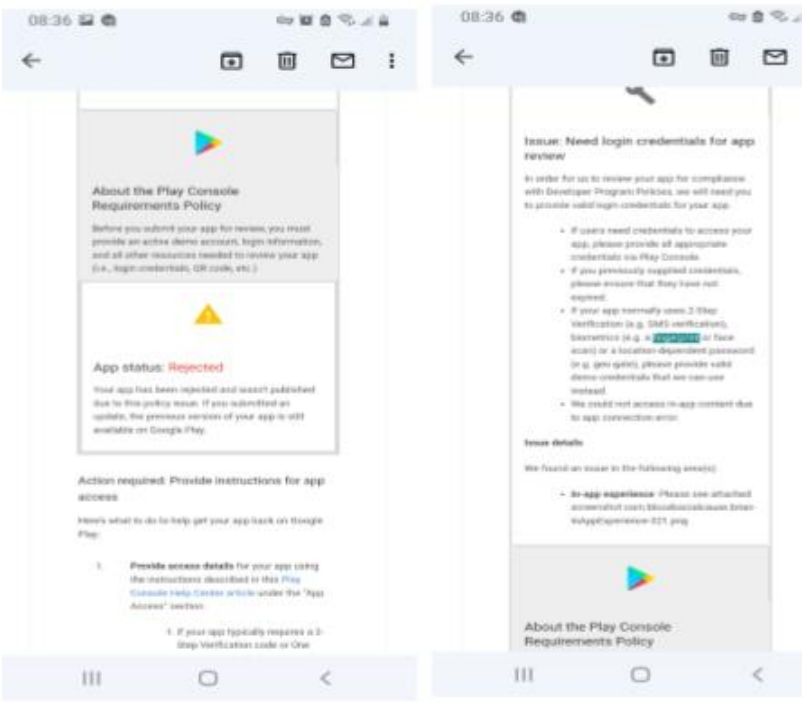

Figure 21: Rejected app draft causes

Developers are expected to give google play service administrators full disclosure of their application function ability, information sharing, and processing before an android application is published on the play store. The information required may include; privacy policies that notify users which information is processed, stored and shared with third parties. Users can only access the application once they have read and agreed to the applicable terms and conditions, as shown in the figure above.

Google Analytics equips developers with real-time analytics on a reporting dashboard on their play account that discloses aspects such as key performance indicators, crashes within the app, and several downloads, among others. From a security perspective, these are useful as if a developer notices a huge drop in the number of downloads, then there could be an issue with the application. If a crash is reported, then the error causing the application bug is updated with a patch that works perfectly to meet user needs.

Conclusion

In conclusion, numerous vulnerabilities exist that expose user information to cyber attackers over the web and mobile applications hosted on active internet connections. The rise in infrastructure leading to internet connectivity over web applications and the technology that supports people's daily life has brought about conflicting interests from cyber attackers who aim to exploit these connected systems. Their skills and techniques to exploit targeted systems rise with technological advancement.

This should encourage and raise awareness by more ethical penetration testers to ensure that more qualified ethical hackers are equipped to secure user data from cyber attackers. Information security effectiveness on a web or mobile application relies on the technology implemented to secure the connected frameworks and server networks that control the application programming interface. Obsolete techniques are likely to be overwhelmed by new attack methods, thus compromising user data; thus, regular updating of the security patches after the penetration assessment test should be implemented.

Links

Website- https://bloodsocialcause.com/

Mobile application- https://play.google.com/store/apps/developer?id=Hrishitva+Patel

Files-

https://www.dropbox.com/s/tw1zipcfdkjs6su/website%20source%20code.zip?dl=0

https://www.dropbox.com/s/k2r65l2agy6btzx/APK%20and%20AAB%20bundle.zip?dl=0

Testing videos- https://www.dropbox.com/s/zqe6z145ihy5my5/videos.zip?dl=0

References

[1]. Kumar, R., Kumar, R., & Tyagi, M. (2021, December). Web Based Online Blood Donation System. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1630-1632). IEEE.

[2]. Chell, K., Davison, T. E., Masser, B., & Jensen, K. (2018). A systematic review of incentives in blood donation. *Transfusion*, *58*(1), 242-254.

[3]. Pratyusha, P. U., Chaitanya, K., Saranam, A., Manideep, K., & Kranthi, S. (2021, October). Smart Intelligent Web-based Online Blood Donation System. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1813-1819). IEEE.

[4]. Ahdan, S., & Setiawansyah, S. (2021). Android-Based Geolocation Technology on a Blood Donation System (BDS) Using the Dijkstra Algorithm. *IJAIT (International Journal of Applied Information Technology)*, *5*(01), 1-15.

[5]. Muhammad, G., Asif, H., Abbas, F., Memon, I., & Fazal, H. (2020). An ERP-Based Blood Donation Management System for Hospitals and Donors. *Sukkur IBA Journal of Emerging Technologies*, *3*(1), 44-54.

[6]. Ali, R. S., Hafez, T. F., Ali, A. B., & Abd-Alsabour, N. (2017, March). Blood bag: A web application to manage all blood donation and transfusion processes. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 2125-2130). IEEE.

[7]. Noori, M. A., Hussien, S. A. S., & Al-Janabi, T. A. (2021). Blood donors appointment booking and managing system using PC and mobile web browsers in the current pandemic (COVID-19). *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(1), 566-574.

[8]. Masser, B., France, C. R., Foot, J., Rozsa, A., Hayman, J., Waller, D., & Hunder, E. (2016). Improving first-time donor attendance rates through the use of enhanced donor preparation materials. *Transfusion*, *56*(6pt2), 1628-1635.

[9]. Boddukuru, H. R., & Cetinkaya, D. (2022). Analysis and Design of an Information System for Blood Component Donations.