IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 8, June 2022

Secured Authentication using Face-Auth

Sagar Mane[1], Tejas Nikumb[2], Digvijaysing Rajput[3], Suved Chougule[4], Mahesh Gaikwad[5]

B.E. Students, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune[1,2,3,4,5]

Abstract: *These days, maximum of the apps is using the traditional technique of username and password device and focusing on how to make passwords extra secured the usage of encryption strategies, however because of day-by-day new vulnerabilities & its limitations, presently many corporations are shifting toward a new manner of Third-party authorization system. We are created new Authentication System as Face Auth Web App System using Biometric Face Recognition, so user can easily Login & Signup using Face Authentication Process which is very secure & easier to use.*

Keywords: Third-Party Authentication, Transport Layer Security (TLS), Privacy, Machine Learning, Face Recognition, etc.

I. INTRODUCTION

With the widespread use of web apps, the need for web application development has skyrocketed in recent years. Online application development has the advantage of allowing new developers with innovative ideas to form teams and create web applications. Vulnerabilities happen as a result of a platform fault or a lack of experience among web developers. Because of the widespread vulnerabilities found in web applications, web application.

II. SECURITY

Security has become a big concern. Attackers have an endless supply of vulnerabilities and payloads to exploit in order to obtain unauthorised access to various web apps. Every time a modification is made to a layer of web application architecture, there is a potential that new vulnerabilities will emerge.

Inexperienced web developers who aren't familiar with secure code principles create applications that are highly vulnerable to attack. When these apps are released without sufficient security testing, they become a tempting target for attackers. Any user who uses such susceptible programmes becomes a target for hackers, exposing their personal information and privacy.

When it comes to designing secure code, a variety of factors come into play, many of which are outside the developers' direct control. That is why typical flaws like SQL injection persist in today's systems, and why application security testing software is so crucial. These issues can be solved - with a little knowledge; businesses can start addressing these issues head on and better equip developers to deal with SQL injection.

There are numerous common vulnerabilities that affect various websites, including:

1. **SQL INJECTION ATTACKS**

   SQL injection is a type of website security flaw / weakness that allows attackers to tamper with a web application's database data queries. It allows the attacker to see the important data that they wouldn't ordinarily be able to see. These include information related to other users or any other information that the app has access to. An attacker can often modify or destroy this data, causing the application's content or behaviour to change permanently.

2. **CROSS SITE SCRIPTING (XSS) ATTACKS**

   Cross-Site Scripting (XSS) attacks are Website injection attacks in which malicious scripts are inserted into innocent websites / Victims Website. XSS attacks occur when an attacker utilises a web application to transmit malicious code to unique end user, typically in the form / Way of a Client-side browser script. The vulnerabilities that permit these attacks to work are common and can be easily found. whenever a web application accepts the user input & its output in their website without pre verification or any encoding.

DOI: 10.48175/IJARSCT-5220

3. **BRUTE FORCE ATTACKS**
   A brute force attack involves guessing login information, encryption keys, or locating a hidden web page by trial and error. Hacker's experiment with every possible combination in the hopes of making the correct guess. These cyber-attacks use 'brute force,' which implies that they try to 'force' their way into your private account by employing tremendous force (s).
4. **SESSION FIXATION ATTACKS**
   An attacker can hijack a valid user session via the Session Fixation technique. The attack focuses on a flaw in the way an online application, specifically the susceptible web application, manages the session ID. When a user is authenticated, no new session ID is assigned, allowing an existing session ID to be used. The attack entails getting a valid session ID (for example, via connecting to the application), convincing a user to authenticate with that session ID, and then hijacking the user-validated session using the session ID. The attacker must provide a legitimate Web application session ID and attempt to use it in the victim's browser.
5. **BROKEN AUTHENTICATION ATTACKS**
   Poorly developed authentication and session management functions are the most common causes of failed authentication. Broken authentication attacks attempt to gain control of one or more accounts by granting the attacker the same privileges as the victim. Authentication and session API management request that are incorrectly implemented / tampered can pose a high security risk for website. If attackers discover these flaws, they may be able to simply assume the identities of legitimate users. Such attacks are the main reason we created our website to help this website to secure from these attacks. Our website is solely based on two systems token authentication and Face reorganization hence these attacks cannot be performed if the website uses our API's.

III. METHODOLOGY

We used two-step authentication systems for this project. The first one is the token system and the second one is the face reorganization system. The User first has to visit our website http://faceauth.tech/ here the user has to register his details. The organization which wants to use our API's can also register on our website. After the user has been registered the user can now use our face authentication validation system.

When new users sign in using our validation framework, our framework will ask for their email address, after which they will receive a token. The framework will activate the device's camera after the user enters the token, which will capture the client image and send it to our ML code Authentication Server. Following successful confirmation, our authentication server will naturally share required User information with the Website that the client was visiting.

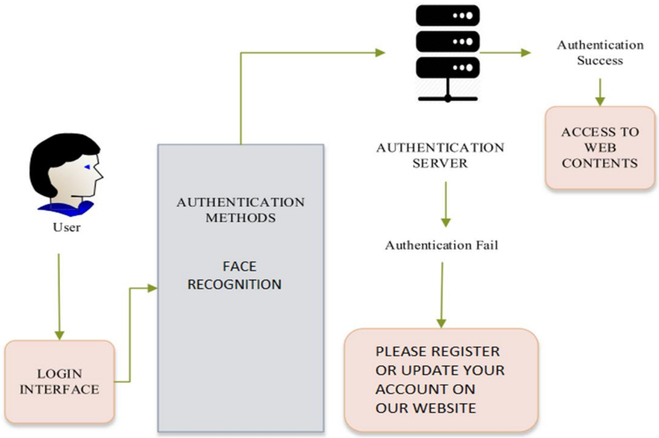


Figure: Flow Diagram

If User Verification fails, it means either the user has not registered on our website, in which case they will be given the option to do so, or they need to update their previous face images on our server for identification purposes, in which case they will be able to log in and update their credentials as needed.

IV. WORKING/ RESULT

First the user has to register on our website to use our facilities. He has to add his personal details such as Name, Email, Password and Phone no.

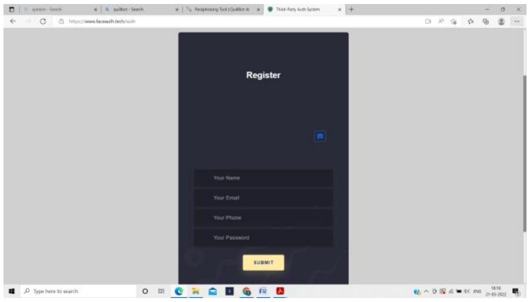


Figure 1: Registration page

After the users account is created the user can now login. The user first has to enter his email Id once the user enters his email a token is sent to the users email Id which he has to enter in the input field. Once the token is accepted the user has to click his picture through his camera. Once the picture is accepted the user is now logged in.

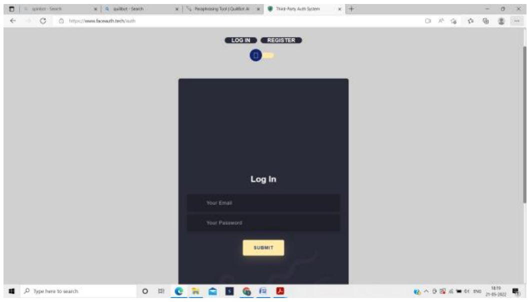
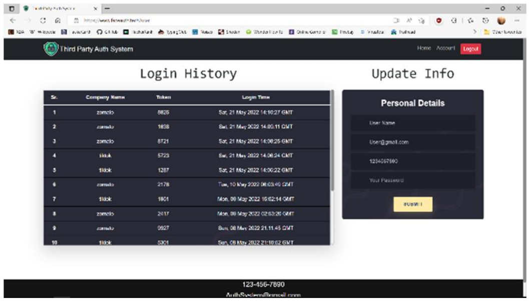


Figure 2: Login page

Once the user is logged in the user can now see his login history to different accounts and can use our facility to login to different website organisations which are registered on our website. The user will also receive his token on this website when he tries to login into a website which is using our API. The user can also update his personal details on this website whenever he feels the need to update it.



Login History

Sr.	Company Name	Token	Login Time
1	zomato	8826	Sat, 21 May 2022 14:10:27 GMT
2	zomato	1838	Sat, 21 May 2022 14:09:11 GMT
3	zomato	8721	Sat, 21 May 2022 14:08:25 GMT
4	tiktok	5723	Sat, 21 May 2022 14:08:24 GMT
5	tiktok	1287	Sat, 21 May 2022 14:06:22 GMT
6	zomato	2178	Tue, 10 May 2022 08:03:49 GMT
7	tiktok	1801	Mon, 09 May 2022 16:02:14 GMT
8	zomato	2417	Mon, 09 May 2022 02:53:20 GMT
9	zomato	0827	Sun, 08 May 2022 21:11:45 GMT
10	tiktok	5301	Sun, 08 May 2022 21:10:52 GMT

Update Info

Personal Details

User Name

User@gmail.com

1234567890

Your Password

SUBMIT

123-456-7890

AuthSystem@gmail.com

Figure 3: Account interface

To demonstrate the application of our API we created a demo website which uses our API to login.

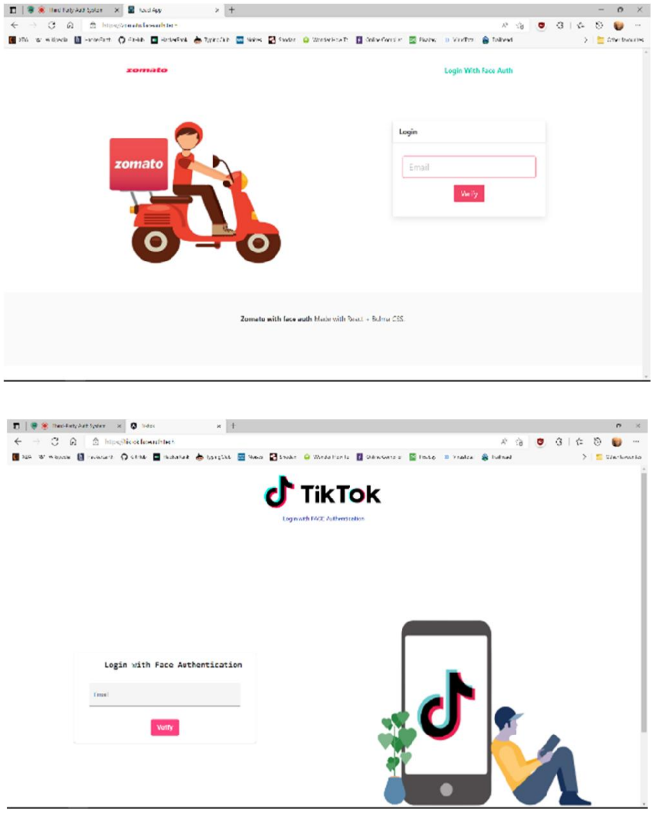
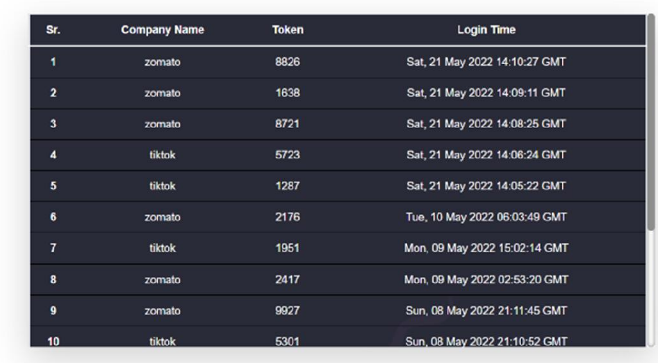

zomato
Login With Face Auth
Login
Email
Verify
Zomato with face auth Made with React + Bulma CSS
TikTok
Login with FACE Authentication
Login with Face Authentication
Email
Verify

Figure 4: Sample Website

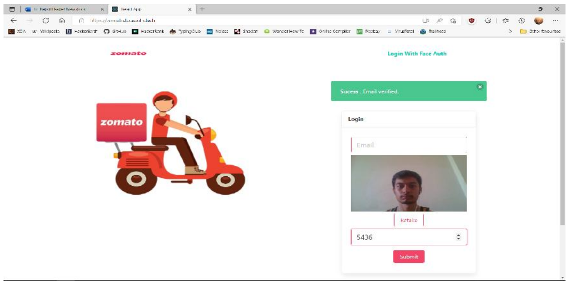
When the user goes to a website which is using our API the user has to enter his email on the website. Once the user enters email on the website the website will send a request to our server for a token and then the user will receive a token on our website which he has to enter on the organisation's website.



Sr.	Company Name	Token	Login Time
1	zomato	8826	Sat, 21 May 2022 14:10:27 GMT
2	zomato	1638	Sat, 21 May 2022 14:09:11 GMT
3	zomato	8721	Sat, 21 May 2022 14:08:25 GMT
4	tiktok	5723	Sat, 21 May 2022 14:06:24 GMT
5	tiktok	1287	Sat, 21 May 2022 14:05:22 GMT
6	zomato	2176	Tue, 10 May 2022 06:03:49 GMT
7	tiktok	1951	Mon, 09 May 2022 15:02:14 GMT
8	zomato	2417	Mon, 09 May 2022 02:53:20 GMT
9	zomato	9927	Sun, 08 May 2022 21:11:45 GMT
10	tiktok	5301	Sun, 08 May 2022 21:10:52 GMT

Figure 5: Token received on our website

When the user enters the token, the camera then captures the user's picture and sends it for validation on our server. If the user is authenticated the user can now successfully login to the organisation's website.



Sucess ..Email verified.

5436

Figure 6: Camera Capture

In such way other organisations can use our website to login to their website without having to worry about login security.

V. CONCLUSION

In this paper, we talked about better approaches for Authentication in site/web administrations and making them safer by adding a strong layer of outsider face validation framework while supplanting customary username and passwords framework. Regardless of whether New Authentication sounds like the ideal framework, comfort, and security across the board bundle. We likewise should be careful with not confiding in any framework indiscriminately without appropriate examination. Since every framework enjoys its own benefits, it likewise holds a critical security defect that conventional username and passwords never needed to make up for.

REFERENCES

[1] Web Application Vulnerabilities Their Exploitation and Prevention. (2020)
[2] Combination RSA with One Time Pad for Enhance Scheme of 2-Factor Authentication. (2020)
[3] Towards Integrated Method of Detection & Description for Face-Authentication System. (2020)
[4] Discussing Alternative Login Methods & Their Advantages & Disadvantages. (2018)
[5] Face & Gender Recognition System based on Convolution Neural networks. (2019)
[6] Study on Face Recognition Techniques. (2020)