Project Report

First Purpose of the Test:Identify vulnerabilities in the OWASP Juice Shop to enhance security.

Key Findings :

- nsitive admin paths were exposed.
- Admin access gained via brute force.
- XSS exploited in search functionality.

Recommendations :

1- Limit login attempts.

2- Sanitize inputs.

3- Secure admin paths.

Scope and Methodology :

- Scope: OWASP Juice Shop web application
- Approach:Black-box testing

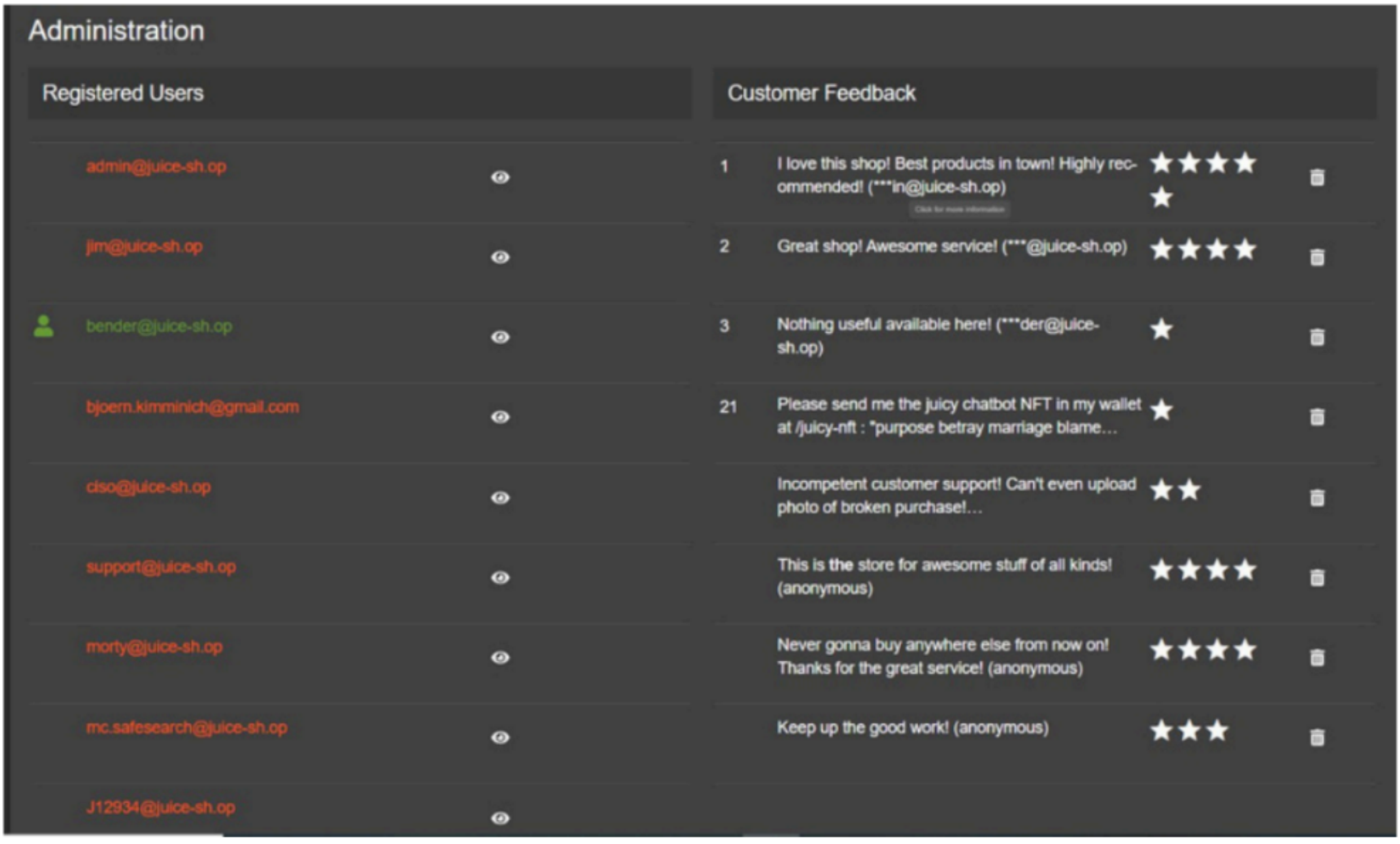
Vulnerability Findings :

1. **Enumeration to Find Admin Path:**

   a) Issue: Exposed /admin path.

   b) Impact: Unauthenticated admin access.

   c) Fix: Hide paths, add authentication.

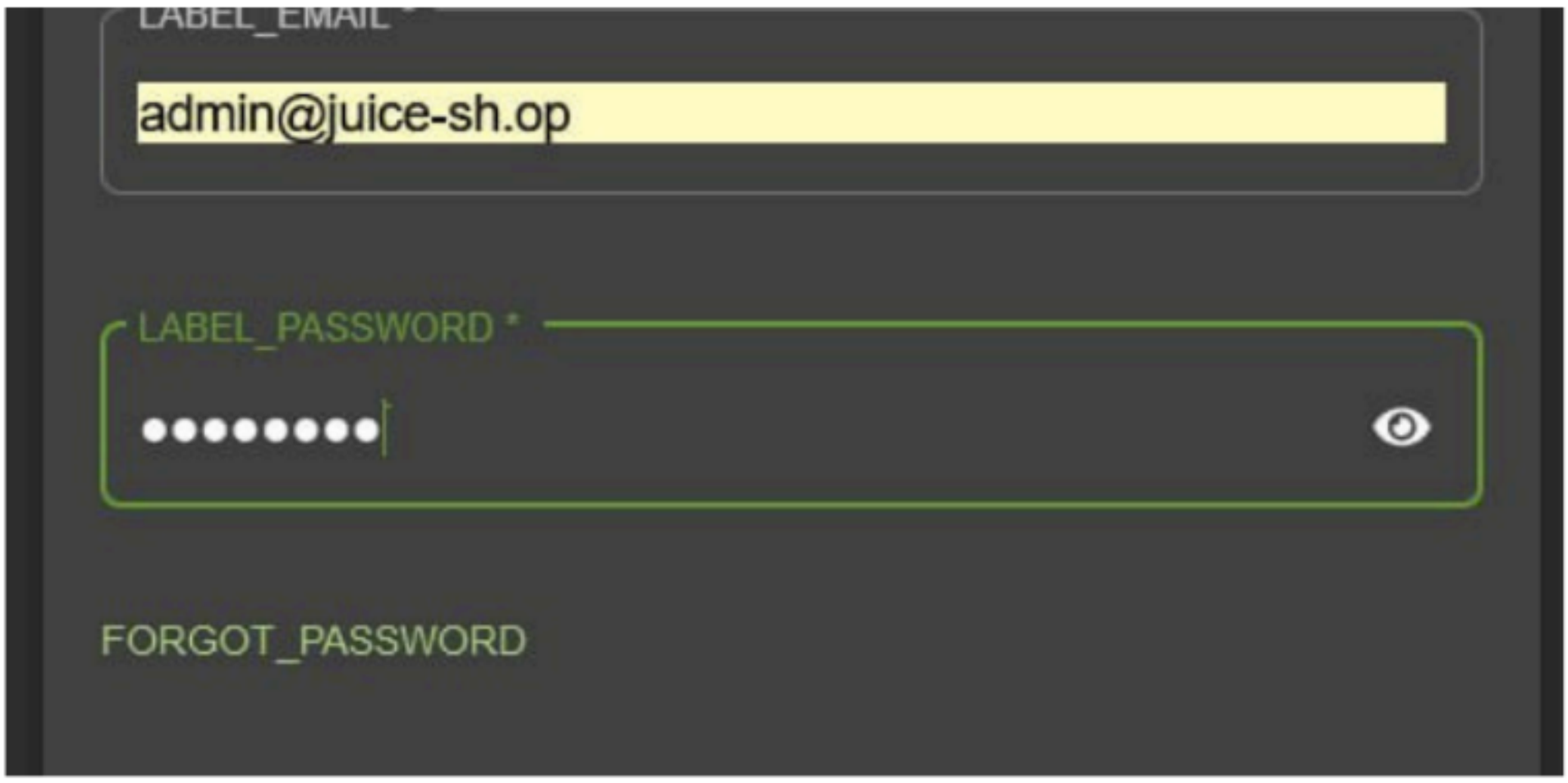


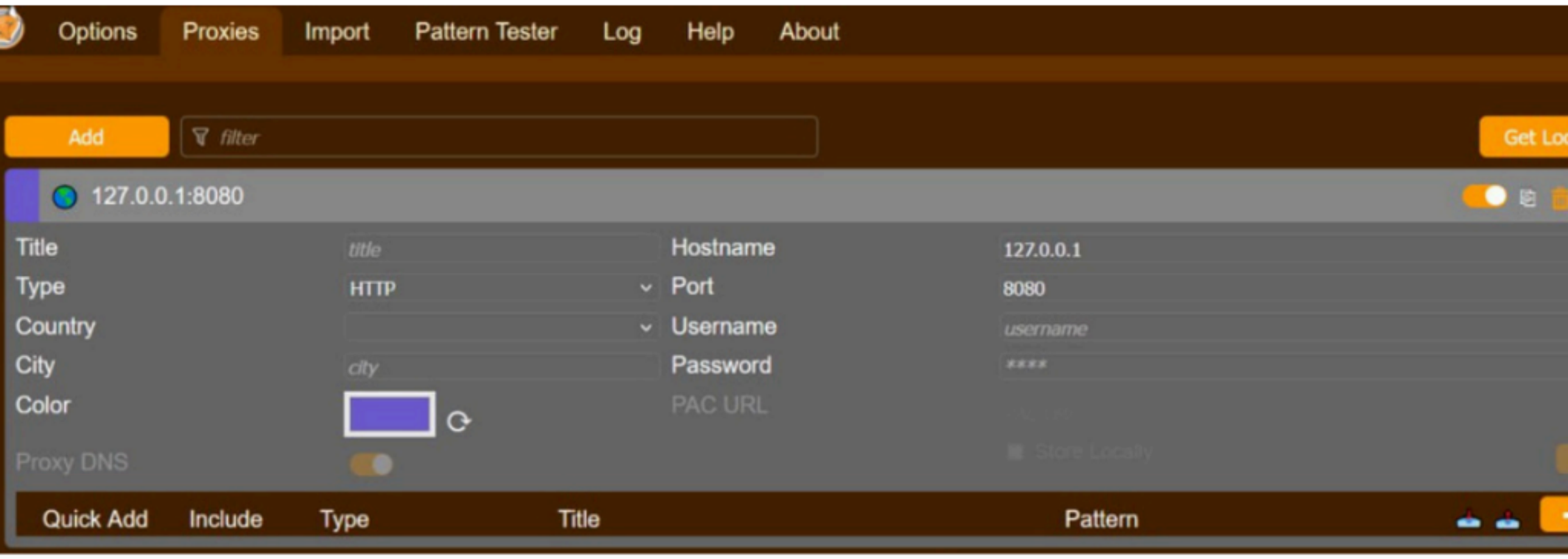
2- Brute Force on Admin Credentials :

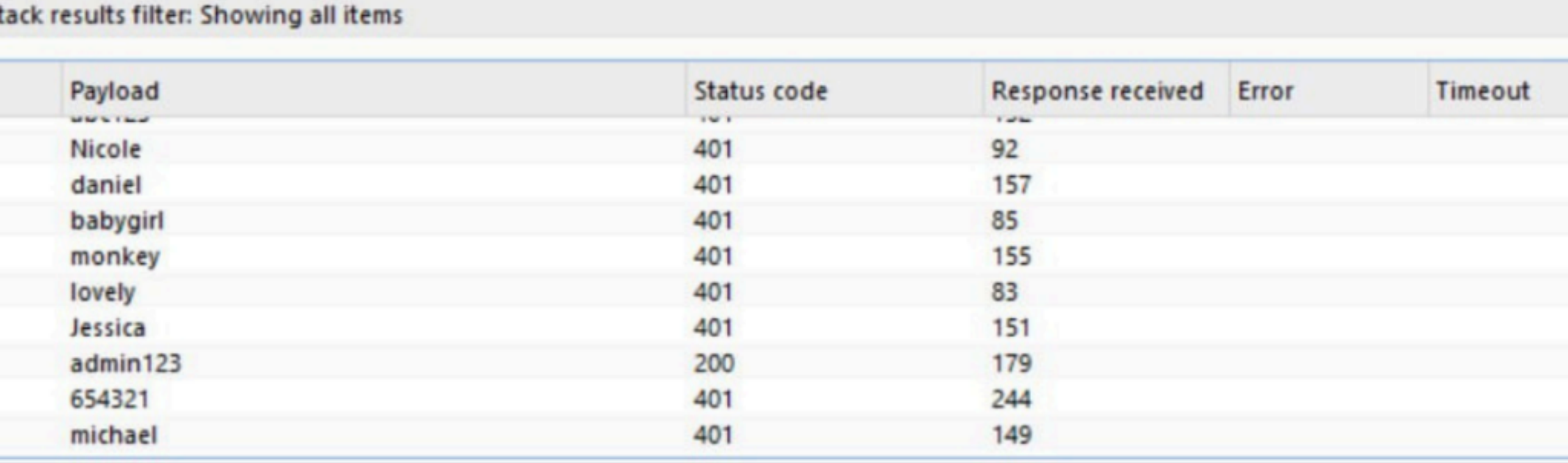
a) Issue: Admin access via brute force.

b) Impact: Full admin privileges.

c) Fix: Track login attempts, lock accounts.





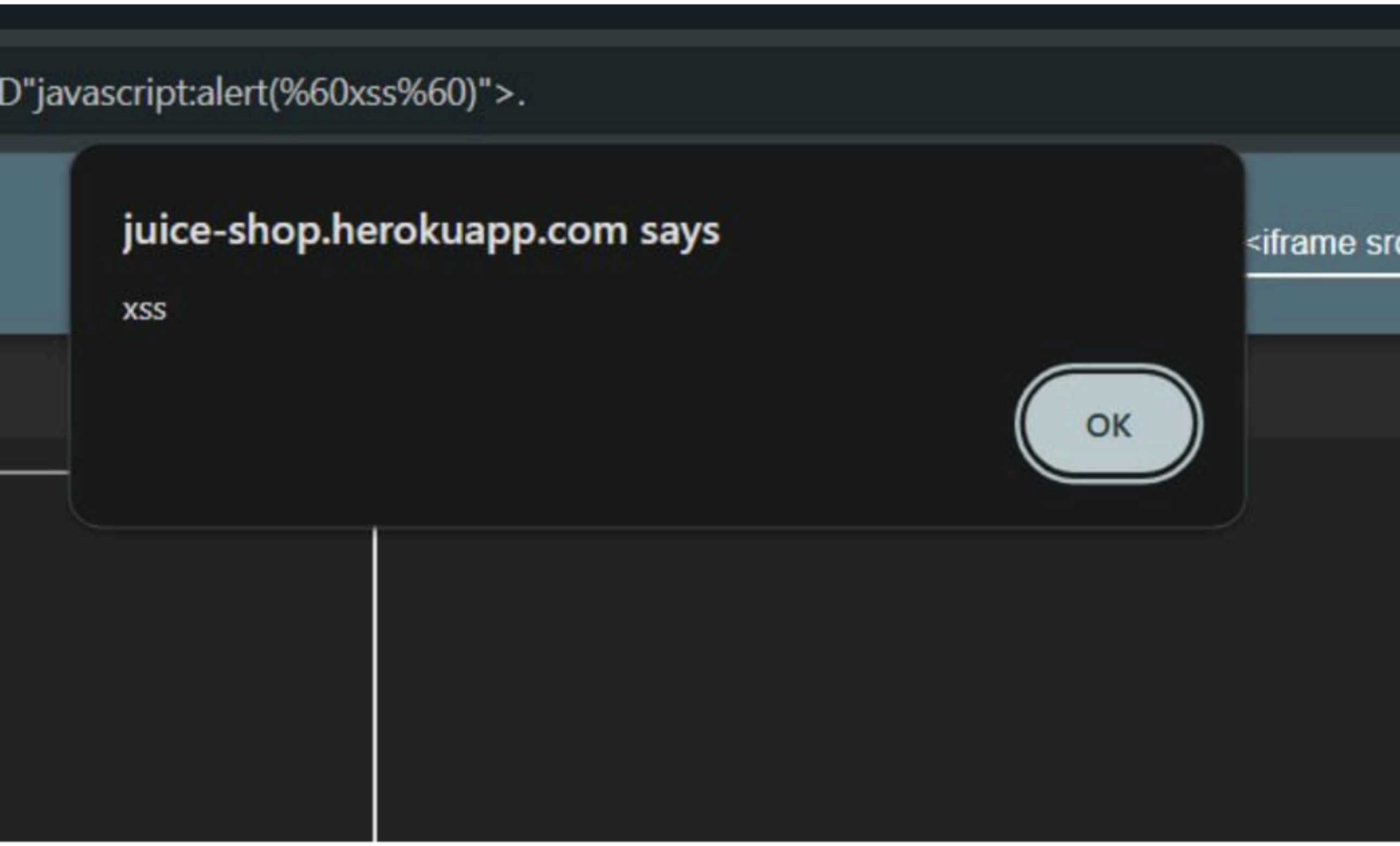


3- XSS in Product Search :

a) Issue: Executable scripts in search.

b) Impact: Data theft, user redirection.

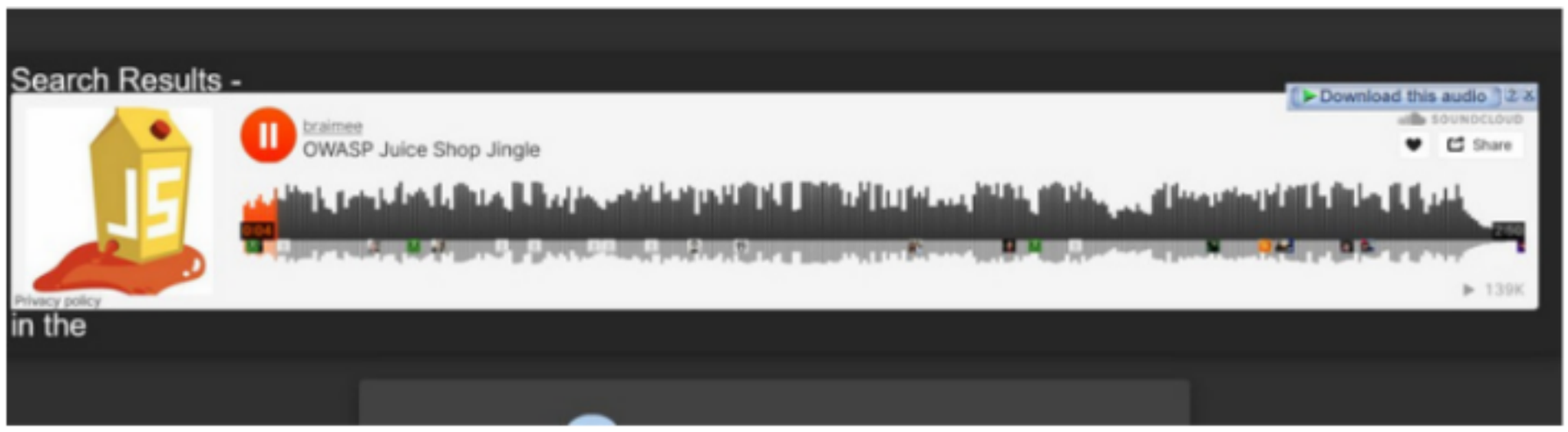
c) Fix: Validate inputs, encode outputs.



Bonus

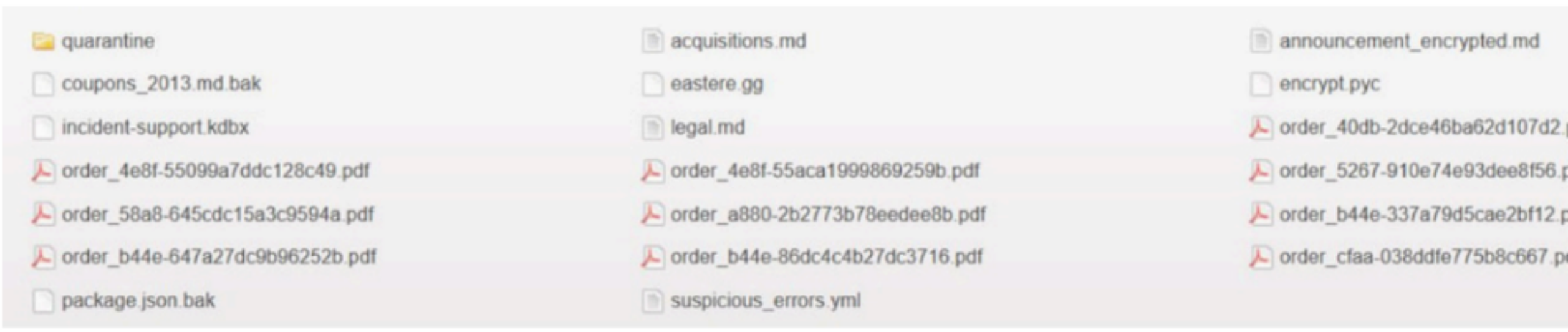
4-Bonus payload :

- It refers to specific data that must be sent in the application to achieve a specific goal such as executing malicious code or obtaining additional information



5-Confidental document

- document within the site that contains sensitive information such as passwords, encryption keys, or internal information



6-Error handling

- A way in which an application handles errors that occur while it is runnin

Exploitation and Attack Simulation

Outcome:

1-Admin panel accessed.

2-Admin credentials compromised.

3-XSS attack demonstrated.

Conclusion

The application has critical vulnerabilities requiring immediate fixes
Regular security reviews are recommended.

Project Team

Abdullah Mohamed 2305028

Hossam allnaser 2305508

Youssef Sobhy 2305033