

Project Report

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

Key Findings :

- Sensitive 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 :

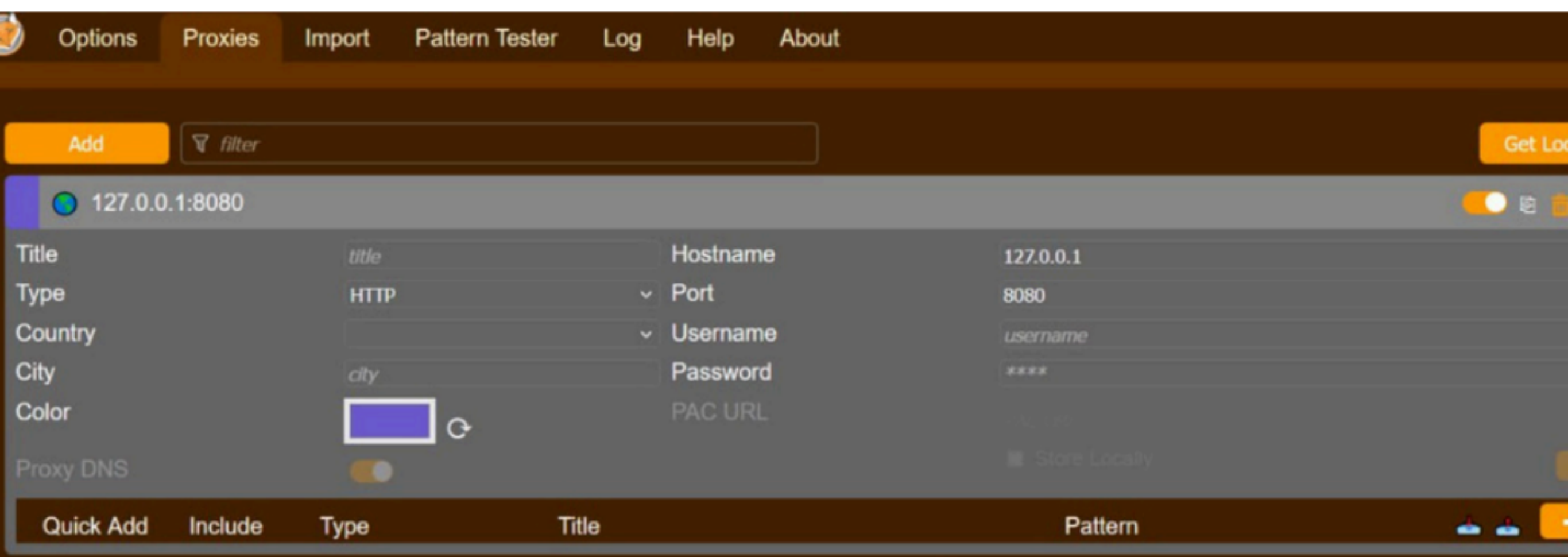
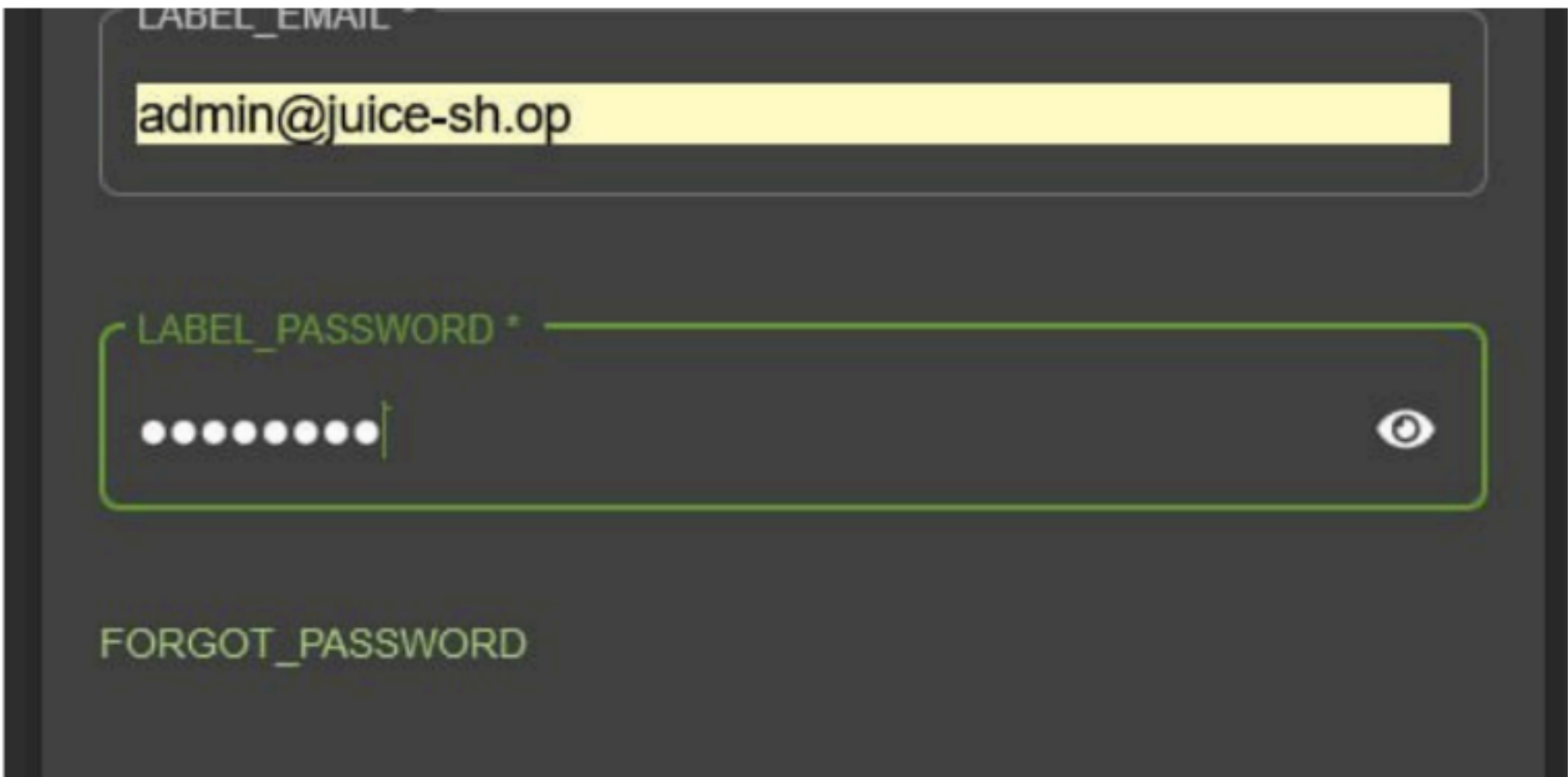
1.Enumeration to Find Admin Path:

- a) Issue: Exposed /admin path.
- b) Impact: Unauthenticated admin access.
- c) Fix: Hide paths, add authentication.

Administration				
Registered Users			Customer Feedback	
admin@juice-sh.op			1 I love this shop! Best products in town! Highly recommended! (**in@juice-sh.op)	★★★★★
jlm@juice-sh.op			2 Great shop! Awesome service! (**@juice-sh.op)	★★★★★
bender@juice-sh.op			3 Nothing useful available here! (**der@juice-sh.op)	★
bjoern.kimminich@gmail.com			21 Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriage blame...	★
ciso@juice-sh.op			Incompetent customer support! Can't even upload photo of broken purchase!...	★★
support@juice-sh.op			This is the store for awesome stuff of all kinds! (anonymous)	★★★★★
morty@juice-sh.op			Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)	★★★★★
mc.safesearch@juice-sh.op			Keep up the good work! (anonymous)	★★★★
J12934@juice-sh.op				

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.



Positions

Attack results filter: Showing all items

Payload	Status code	Response received	Error	Timeout
Nicole	401	92		
daniel	401	157		
babygirl	401	85		
monkey	401	155		
lovely	401	83		
Jessica	401	151		
admin123	200	179		
654321	401	244		
michael	401	149		

3- XSS in Product Search :

- a) Issue: Executable scripts in search.
- b) Impact: Data theft, user redirection.
- c) Fix: Validate inputs, encode outputs.

D"javascript:alert(%60xss%60)">.

juice-shop.herokuapp.com says

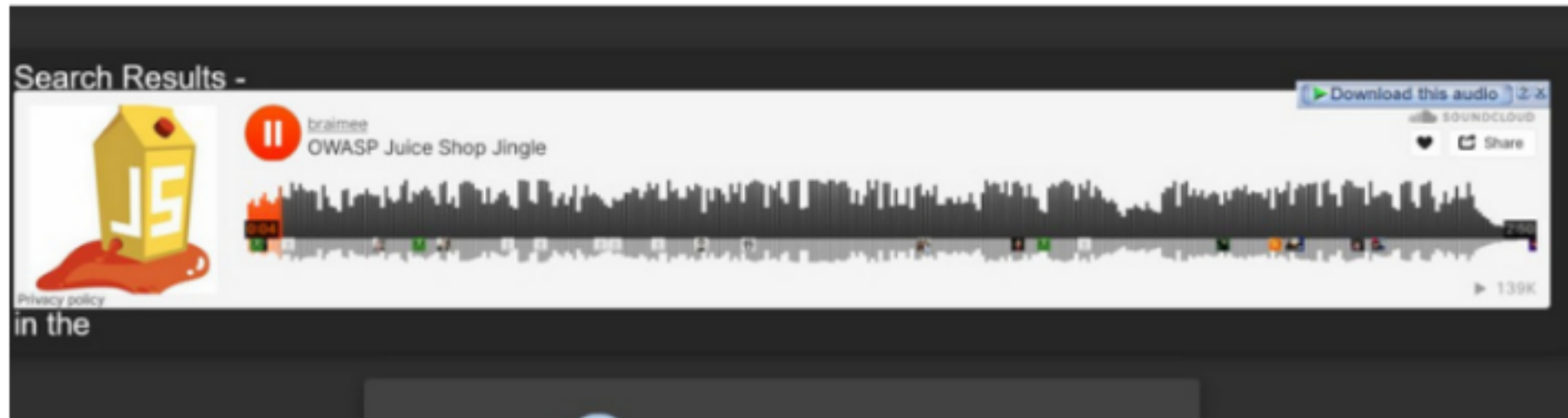
xss

OK

Bonus

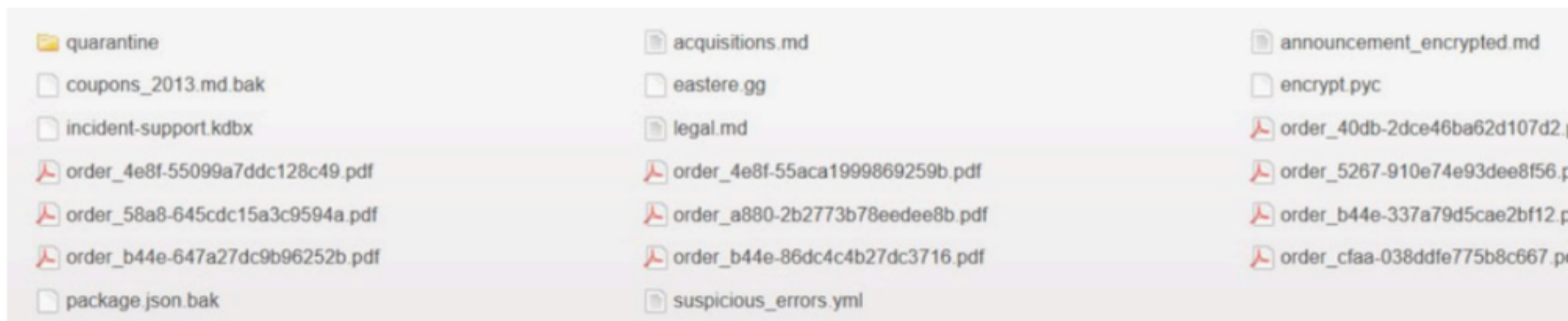
4-Bonus payload :

- 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



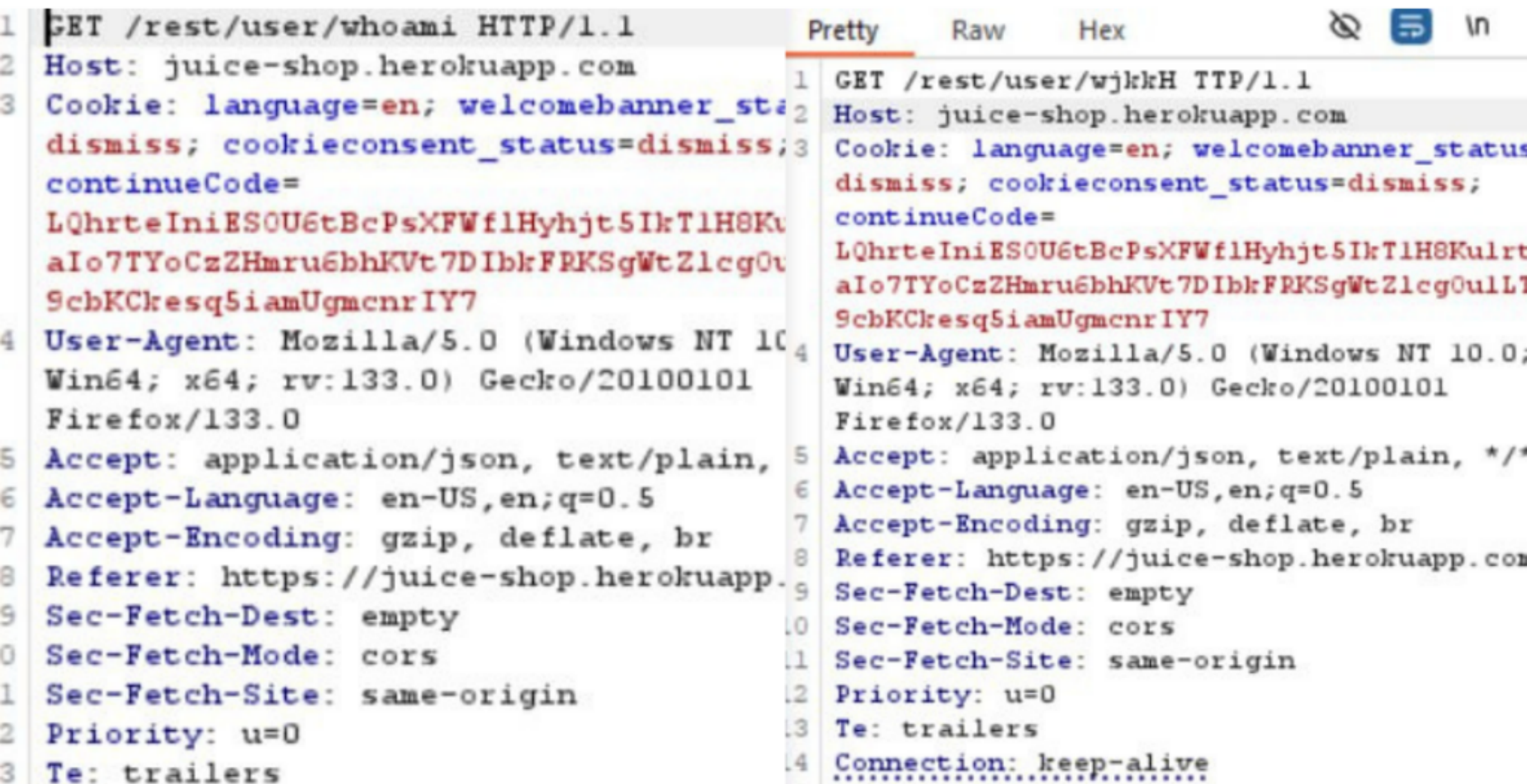
5-Confidential document

- 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 running



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