

# VAPT Report

## Executive Summary

This report outlines the findings from the recent Vulnerability Assessment and Penetration Testing (VAPT) engagement. The following sections detail the vulnerabilities identified, their impact, and recommendations for remediation.

## Directory traversal

1. URL: <https://35.212.180.132> - Result: 200
2. URL: [https://35.212.180.132/product\\_page.php?id=74](https://35.212.180.132/product_page.php?id=74) - Result: 200
3. URL: [https://35.212.180.132/product\\_page.php?id=23](https://35.212.180.132/product_page.php?id=23) - Result: 200
4. URL: [https://35.212.180.132/product\\_page.php?id=57](https://35.212.180.132/product_page.php?id=57) - Result: 200
5. URL: [https://35.212.180.132/product\\_page.php?id=14](https://35.212.180.132/product_page.php?id=14) - Result: 200
6. URL: [https://35.212.180.132/new\\_listing.php](https://35.212.180.132/new_listing.php) - Result: 200
7. URL: [https://35.212.180.132/product\\_page.php?id=55](https://35.212.180.132/product_page.php?id=55) - Result: 200
8. URL: <https://35.212.180.132/aboutus.php> - Result: 200
9. URL: <https://35.212.180.132/customerservice.php> - Result: 200
10. URL: <https://35.212.180.132/index.php> - Result: 200
11. URL: <https://35.212.180.132/findus.php> - Result: 200
12. URL: [https://35.212.180.132/product\\_page.php?id=61](https://35.212.180.132/product_page.php?id=61) - Result: 200
13. URL: <https://35.212.180.132/listings.php> - Result: 200
14. URL: [https://35.212.180.132/transaction\\_history.php](https://35.212.180.132/transaction_history.php) - Result: 200
15. URL: [https://35.212.180.132/product\\_page.php?id=68](https://35.212.180.132/product_page.php?id=68) - Result: 200
16. URL: <https://35.212.180.132/logout.php> - Result: 200
17. URL: [https://35.212.180.132/product\\_page.php?id=58](https://35.212.180.132/product_page.php?id=58) - Result: 200

# VAPT Report

18. URL: <https://35.212.180.132/console.php> - Result: 200
19. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=19](https://35.212.180.132/shopping_cart.php?user_id=19) - Result: 200
20. URL: [https://35.212.180.132/profile.php?account\\_id=19](https://35.212.180.132/profile.php?account_id=19) - Result: 200
21. URL: [https://35.212.180.132/product\\_page.php?id=35](https://35.212.180.132/product_page.php?id=35) - Result: 200
22. URL: <https://35.212.180.132/login.php> - Result: 200
23. URL: <https://35.212.180.132/robots.txt> - Result: 200
24. URL: <https://35.212.180.132/uploads> - Result: 200
25. URL: <https://35.212.180.132/api> - Result: 200
26. URL: <https://35.212.180.132/login.php> - Result: login
27. URL: <https://35.212.180.132/api> - Result: api

## Forced-browsing

No findings reported.

## Idor

1. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=6](https://35.212.180.132/shopping_cart.php?user_id=6) - Result: idor
2. URL: [https://35.212.180.132/profile.php?account\\_id=5](https://35.212.180.132/profile.php?account_id=5) - Result: idor
3. URL: [https://35.212.180.132/profile.php?account\\_id=6](https://35.212.180.132/profile.php?account_id=6) - Result: idor
4. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=7](https://35.212.180.132/shopping_cart.php?user_id=7) - Result: idor
5. URL: [https://35.212.180.132/profile.php?account\\_id=3](https://35.212.180.132/profile.php?account_id=3) - Result: idor
6. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=1](https://35.212.180.132/shopping_cart.php?user_id=1) - Result: idor
7. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=5](https://35.212.180.132/shopping_cart.php?user_id=5) - Result: idor
8. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=9](https://35.212.180.132/shopping_cart.php?user_id=9) - Result: idor

# VAPT Report

- 9. URL: [https://35.212.180.132/profile.php?account\\_id=1](https://35.212.180.132/profile.php?account_id=1) - Result: idor
- 10. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=4](https://35.212.180.132/shopping_cart.php?user_id=4) - Result: idor
- 11. URL: [https://35.212.180.132/profile.php?account\\_id=2](https://35.212.180.132/profile.php?account_id=2) - Result: idor
- 12. URL: [https://35.212.180.132/profile.php?account\\_id=8](https://35.212.180.132/profile.php?account_id=8) - Result: idor
- 13. URL: [https://35.212.180.132/profile.php?account\\_id=7](https://35.212.180.132/profile.php?account_id=7) - Result: idor
- 14. URL: [https://35.212.180.132/product\\_page.php?id=17](https://35.212.180.132/product_page.php?id=17) - Result: idor
- 15. URL: [https://35.212.180.132/product\\_page.php?id=14](https://35.212.180.132/product_page.php?id=14) - Result: idor
- 16. URL: [https://35.212.180.132/product\\_page.php?id=23](https://35.212.180.132/product_page.php?id=23) - Result: idor
- 17. URL: [https://35.212.180.132/profile.php?account\\_id=4](https://35.212.180.132/profile.php?account_id=4) - Result: idor
- 18. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=2](https://35.212.180.132/shopping_cart.php?user_id=2) - Result: idor
- 19. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=3](https://35.212.180.132/shopping_cart.php?user_id=3) - Result: idor
- 20. URL: [https://35.212.180.132/shopping\\_cart.php?user\\_id=8](https://35.212.180.132/shopping_cart.php?user_id=8) - Result: idor
- 21. URL: [https://35.212.180.132/profile.php?account\\_id=9](https://35.212.180.132/profile.php?account_id=9) - Result: idor

## Api-idor

No findings reported.

## Weak api controls - unauthenticated

No findings reported.

## Weak api controls - authenticated

No findings reported.

## Session management

No findings reported.

# VAPT Report

## Conclusion & Recommendations

Based on the findings, immediate remediation actions are recommended to mitigate the identified vulnerabilities. A detailed remediation plan should be developed and executed to improve the overall security posture.