BrokenAXE: Broken Access Control Toolkit

Vulnerability Assessment & Penetration Testing

Report Date: 2025-03-03

Target: 35.212.180.132

VAPT Report - BrokenAXE

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 & Heuristic scanning

Directory & Heuristic Scanning is a web vulnerability assessment technique combining forced browsing and intelligent content analysis. Forced browsing uses a wordlist to systematically identify hidden directories and files on a web server, exposing resources not directly linked or indexed. Meanwhile, heuristic scanning analyzes web pages, HTTP headers, meta tags, and scripts to detect technologies, misconfigurations, and vulnerabilities like injection flaws or insecure object references.

1. URL: https://35.212.180.132 - Result: 200
2. URL: https://35.212.180.132/customerservice.php - Result: 200
3. URL: https://35.212.180.132/listings.php - Result: 200
4. URL: https://35.212.180.132/product_page.php?id=23 - Result: 200
5. URL: https://35.212.180.132/product_page.php?id=35 - Result: 200
6. URL: https://35.212.180.132/product_page.php?id=74 - Result: 200
7. URL: https://35.212.180.132/index.php - Result: 200
8. URL: https://35.212.180.132/product_page.php?id=55 - Result: 200
9. URL: https://35.212.180.132/product_page.php?id=61 - Result: 200
10. URL: https://35.212.180.132/transaction_history.php - Result: 200
11. URL: https://35.212.180.132/findus.php - Result: 200
12. URL: https://35.212.180.132/profile.php?account_id=19 - Result: 200
13. URL: https://35.212.180.132/product_page.php?id=58 - Result: 200
14. URL: https://35.212.180.132/product_page.php?id=68 - Result: 200
15. URL: https://35.212.180.132/new_listing.php - Result: 200
16. URL: https://35.212.180.132/aboutus.php - Result: 200
17. URL: https://35.212.180.132/shopping_cart.php?user_id=19 - Result: 200
18. URL: https://35.212.180.132/logout.php - Result: 200
19. URL: https://35.212.180.132/product_page.php?id=14 - Result: 200
20. URL: https://35.212.180.132/console.php - Result: 200
21. URL: https://35.212.180.132/product_page.php?id=57 - 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/api - Result: api
27. URL: https://35.212.180.132/login.php - Result: login

Insecure Direct Object Reference (IDOR)

Insecure Direct Object Reference (IDOR) is a web application vulnerability where an attacker can access unauthorized resources by manipulating object references. By changing parameters or URLs, an attacker can bypass access controls and view sensitive data or perform unauthorized actions.

1. URL: https://35.212.180.132/profile.php?account_id=2 - Result: idor
2. URL: https://35.212.180.132/shopping_cart.php?user_id=2 - Result: idor
3. URL: https://35.212.180.132/shopping_cart.php?user_id=7 - Result: idor
4. URL: https://35.212.180.132/profile.php?account_id=3 - Result: idor
5. URL: https://35.212.180.132/product_page.php?id=23 - Result: idor
6. URL: https://35.212.180.132/shopping_cart.php?user_id=9 - Result: idor
7. URL: https://35.212.180.132/shopping_cart.php?user_id=3 - Result: idor
8. URL: https://35.212.180.132/profile.php?account_id=5 - Result: idor
9. URL: https://35.212.180.132/shopping_cart.php?user_id=1 - Result: idor
10. URL: https://35.212.180.132/shopping_cart.php?user_id=4 - Result: idor
11. URL: https://35.212.180.132/product_page.php?id=17 - Result: idor
12. URL: https://35.212.180.132/shopping_cart.php?user_id=8 - Result: idor
13. URL: https://35.212.180.132/profile.php?account_id=1 - Result: idor
14. URL: https://35.212.180.132/shopping_cart.php?user_id=6 - Result: idor
15. URL: https://35.212.180.132/product_page.php?id=14 - Result: idor
16. URL: https://35.212.180.132/profile.php?account_id=6 - Result: idor
17. URL: https://35.212.180.132/profile.php?account_id=9 - Result: idor
18. URL: https://35.212.180.132/profile.php?account_id=8 - Result: idor
19. URL: https://35.212.180.132/shopping_cart.php?user_id=5 - Result: idor
20. URL: https://35.212.180.132/profile.php?account_id=7 - Result: idor
21. URL: https://35.212.180.132/profile.php?account_id=4 - Result: idor

API-IDOR

API Insecure Direct Object Reference (API-IDOR) is a vulnerability in an application programming interface (API) that allows attackers to access unauthorized resources by manipulating object references. By changing parameters or URLs, an attacker can bypass access controls and view

sensitive data or perform unauthorized actions.

1. URL: https://35.212.180.132/api/cart/?user_id=9 - Result: api-idor
2. URL: https://35.212.180.132/api/profile/?account_id=8 - Result: api-idor
3. URL: https://35.212.180.132/api/profile/?account_id=4 - Result: api-idor
4. URL: https://35.212.180.132/api/cart/?user_id=20 - Result: api-idor
5. URL: https://35.212.180.132/api/profile/?account_id=21 - Result: api-idor
6. URL: https://35.212.180.132/api/profile/?account_id=6 - Result: api-idor
7. URL: https://35.212.180.132/api/cart/?user_id=2 - Result: api-idor
8. URL: https://35.212.180.132/api/profile/?account_id=9 - Result: api-idor
9. URL: https://35.212.180.132/api/profile/?account_id=20 - Result: api-idor
10. URL: https://35.212.180.132/api/profile/?account_id=3 - Result: api-idor
11. URL: https://35.212.180.132/api/profile/?account_id=2 - Result: api-idor

Weak API Controls - Authenticated

Weak API Controls - Authenticated refers to vulnerabilities in an application programming interface (API) that allow unauthorized access or actions even after authentication. Attackers can exploit these weaknesses to access sensitive data or perform unauthorized operations.

1. URL: https://35.212.180.132/api/profile/?account_id=19 - Result: weak API controls - authenticated
2. URL: https://35.212.180.132/api/cart/?user_id=19 - Result: weak API controls - authenticated

VAPT Report - BrokenAXE

Conclusion & Recommendations

Based on the findings, the following remediation actions are recommended to address the vulnerabilities discovered on the target:

Directory & Heuristic Scanning / Forced Browsing:

1. Harden server configurations by disabling directory listings and removing unnecessary files.
2. Implement strict access controls on directories and files to restrict unauthorized access.
3. Deploy a Web Application Firewall (WAF) to monitor and block malicious requests.

Insecure Direct Object Reference (IDOR):

1. Enforce robust authorization checks to ensure users access only permitted resources.
2. Replace direct object references with indirect tokens that do not expose internal IDs.
3. Conduct regular security audits to validate access controls.

API Insecure Direct Object Reference (API-IDOR):

1. Implement strict authentication and authorization checks on API endpoints.
2. Ensure API responses do not expose sensitive or predictable object references.
3. Validate user access for each API request to prevent unauthorized data exposure.

Weak API Controls - Authenticated:

1. Ensure authenticated users have appropriate permissions.
2. Use session management best practices to prevent token reuse or hijacking.
3. Regularly audit API logs for any signs of abuse.

VAPT Report - BrokenAXE

Summary of Discovered Vulnerabilities

Directory & Heuristic scanning: 27 vulnerability(s) discovered.

Forced Browsing: 0 vulnerability(s) discovered.

Insecure Direct Object Reference (IDOR): 21 vulnerability(s) discovered.

API-IDOR: 11 vulnerability(s) discovered.

Weak API Controls - Unauthenticated: 0 vulnerability(s) discovered.

Weak API Controls - Authenticated: 2 vulnerability(s) discovered.

Session Management: 0 vulnerability(s) discovered.

Total vulnerabilities discovered: 61