

BAC Report - <http://localhost:8082> Broken Access Control Report Site: <http://localhost:8082> Date: 2025-09-09\_10-04-11 Note: Crawled 5 links successfully. Discovered links: <http://localhost:8082/js/html5.js> [http://localhost:8082/user\\_new.php](http://localhost:8082/user_new.php) <http://localhost:8082/info.php> <http://localhost:8082/training.php> <http://localhost:8082/login.php> Summary Total Tests: 10 Total Findings: 35 Vulnerable: 5 IDOR URL Status Risk Details Mitigation - No IDOR parameters found Low No query parameters discovered Use UUIDs or indirect references, enforce access checks on every request. - No IDOR parameters found Low No query parameters discovered Use UUIDs or indirect references, enforce access checks on every request. - No IDOR parameters found Low No query parameters discovered Use UUIDs or indirect references, enforce access checks on every request. - No IDOR parameters found Low No query parameters discovered Use UUIDs or indirect references, enforce access checks on every request. - No IDOR parameters found Low No query parameters discovered Use UUIDs or indirect references, enforce access checks on every request. Path IDOR URL Status Risk Details Mitigation - No numeric path segments Low - General best practices - No numeric path segments Low - General best practices - No numeric path segments Low - General best practices - No numeric path segments Low - General best practices Privilege Escalation URL Status Risk Details Mitigation - Skipped Medium No admin credentials provided Enforce server-side RBAC, never rely on client-side checks. Directory Traversal URL Status Risk Details Mitigation <http://localhost:8082/..etc/passwd> Not Vulnerable High No sensitive content detected (HTTP 404) Sanitize inputs, deny '..', use path whitelisting. <http://localhost:8082/../../admin/config> Not Vulnerable High No sensitive content detected (HTTP 404) Sanitize inputs, deny '..', use path whitelisting. Method Bypass URL Status Risk Details Mitigation <http://localhost:8082/js/html5.js> Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. [http://localhost:8082/user\\_new.php](http://localhost:8082/user_new.php) Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. [http://localhost:8082/user\\_new.php](http://localhost:8082/user_new.php) Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. <http://localhost:8082/info.php> Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. <http://localhost:8082/training.php> Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. <http://localhost:8082/login.php> Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. <http://localhost:8082/login.php> Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. Force Browsing URL Status Risk Details Mitigation <http://localhost:8082/admin> Vulnerable Medium Sensitive page accessible without login Enforce authentication/authorization on all sensitive endpoints. <http://localhost:8082/config> Not Vulnerable Medium Access blocked or redirected (HTTP 404) Enforce authentication/authorization on all sensitive endpoints. <http://localhost:8082/debug> Not Vulnerable Medium Access blocked or redirected (HTTP 404) Enforce authentication/authorization on all sensitive endpoints. <http://localhost:8082/private> Not Vulnerable Medium Access blocked or redirected (HTTP 404) Enforce authentication/authorization on all sensitive endpoints. Header/Token Tampering URL Status Risk Details Mitigation <http://localhost:8082/admin> Vulnerable High Bypassed authorization using missing/forged token Validate tokens strictly server-side; never trust missing or forged headers. <http://localhost:8082/config> Not Vulnerable High Authorization header enforced Validate tokens strictly server-side; never trust missing or forged headers. <http://localhost:8082/private> Not Vulnerable High Authorization header enforced Validate tokens strictly server-side; never trust missing or forged headers. Cookie Manipulation URL Status Risk Details Mitigation <http://localhost:8082/admin> Vulnerable High Cookie manipulation bypassed access Do not store roles in cookies; enforce all roles and permissions server-side. <http://localhost:8082/config> Not Vulnerable High Cookies required and validated Do not store roles in cookies; enforce all roles and permissions server-side. CORS Misconfiguration URL Status Risk Details Mitigation <http://localhost:8082> Not Vulnerable Medium CORS restricted properly Restrict CORS Access-Control-Allow-Origin to trusted domains only. Unauthenticated Access URL Status Risk Details Mitigation <http://localhost:8082/js/html5.js> Vulnerable High Accessible without authentication General best practices [http://localhost:8082/user\\_new.php](http://localhost:8082/user_new.php) Info Low Ambiguous unauth response (HTTP 200) General best practices <http://localhost:8082/info.php> Info Low Ambiguous unauth response (HTTP 200) General best practices <http://localhost:8082/training.php> Info Low Ambiguous

unauth response (HTTP 200) General best practices <http://localhost:8082/login.php> Info Low  
Ambiguous unauth response (HTTP 200) General best practices