BAC Report - http://localhost:8082 Broken Access Control Report Site: http://localhost:8082 Date: 2025-09-09_02-21-45 Note: Crawled 19 links successfully.Discovered links:http://localhost:8082/images/zap.pnghttp://localhost:8082/info.phphttp://localhost:8082/images/twitter.pnghttp://localhost:8082/images/linkedin.pnghttp://localhost:8082/images/owasp.pnghttp://localhost:8082/stylesheets/stylesheet.css http://localhost:8082/images/bee_1.pnghttp://localhost:8082/login.phphttp://localhost:8082/images/favicon.icohttp://localhost:8082/images/blogger.pnghttp://localhost:8082/training.phphttp://localhost:8082/js/html5.jshttp://localhost:8082/user_new.phphttp://localhost:8082/images/cc.pnghttp://localhost:8082/images/netsparker.pnghttp://localhost:8082/images/facebook.pnghttp://localhost:8082/images/netsparker.gifhttp://localhost:8082/images/mk.pnghttp://localhost:8082/images/mme.png Summary Total Tests: 10 Total Findings: 85 Vulnerable: 29 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. - 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. - 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. - 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 - 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 - 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 - 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 - 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/images/zap.png Vulnerable Medium Endpoint accepted POST (possible bypass) 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/images/twitter.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/linkedin.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/owasp.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/stylesheets/stylesheet.css Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/bee_1.png Vulnerable Medium Endpoint accepted POST (possible bypass) 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/images/favicon.ico Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/blogger.png Vulnerable Medium Endpoint accepted POST (possible bypass) 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/js/html5.js Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user_new.php Not Vulnerable Medium Rejected (HTTP 200) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/cc.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/netsparker.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/facebook.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/netsparker.gif Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/mk.png Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images/mme.png Vulnerable Medium Endpoint accepted POST (possible bypass) 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/images/zap.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/info.php Info Low Ambiguous unauth response (HTTP 200) General best practices http://localhost:8082/images/twitter.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/images/linkedin.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/images/owasp.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/stylesheets/stylesheet.css Vulnerable High Accessible without authentication General best practices http://localhost:8082/images/bee_1.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/login.php Info Low Ambiguous unauth response (HTTP 200) General best practices http://localhost:8082/images/favicon.ico Vulnerable High Accessible without authentication General best practices http://localhost:8082/images/blogger.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/training.php Info Low Ambiguous unauth response (HTTP 200) General best practices http://localhost:8082/js/html5.js Vulnerable High Accessible without authentication General best practices http://localhost:8082/user_new.php Info Low Ambiguous unauth response (HTTP 200) General best practices http://localhost:8082/images/cc.png Vulnerable High Accessible without authentication General best practices http://localhost:8082/images/netsparker.png Vulnerable High Accessible without authentication General best practices