BAC Report - http://localhost:8082/xss_get.php Broken Access Control Report Site: http://localhost:8082/xss_get.php Date: 2025-09-09_08-19-08 Note: Crawled 50 links successfully.Discovered links:http://localhost:8082http://localhost:8082/homehttp://localhost:8082/index http://localhost:8082/mainhttp://localhost:8082/dashboardhttp://localhost:8082/adminhttp://localhost:8082/loginhttp://localhost:8082/logouthttp://localhost:8082/profilehttp://localhost:8082/accounthttp://localhost:8082/settingshttp://localhost:8082/confighttp://localhost:8082/usershttp://localhost:8082/userhttp://localhost:8082/apihttp://localhost:8082/api/usershttp://localhost:8082/api/adminhttp://localhost:8082/api/v1http://localhost:8082/managementhttp://localhost:8082/panelhttp://localhost:8082/controlhttp://localhost:8082/searchhttp://localhost:8082/helphttp://localhost:8082/abouthttp://localhost:8082/contacthttp://localhost:8082/registerhttp://localhost:8082/signuphttp://localhost:8082/signinhttp://localhost:8082/forgot http://localhost:8082/resethttp://localhost:8082/change-passwordhttp://localhost:8082/edit-profilehttp://localhost:8082/preferenceshttp://localhost:8082/notificationshttp://localhost:8082/messageshttp://localhost:8082/inboxhttp://localhost:8082/reportshttp://localhost:8082/analyticshttp://localhost:8082/logshttp://localhost:8082/admin/usershttp://localhost:8082/admin/settingshttp://localhost:8082/admin/reportshttp://localhost:8082/admin/logshttp://localhost:8082/user/profilehttp://localhost:8082/user/settingshttp://localhost:8082/user/dashboardhttp://localhost:8082/user/accounthttp://localhost:8082/documentshttp://localhost:8082/imageshttp://localhost:8082/passwords Summary Total Tests: 10 Total Findings: 165 Vulnerable: 4 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. - 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. - 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 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/xss_get.php/../etc/passwd Not Vulnerable High No sensitive content detected (HTTP 404) Sanitize inputs, deny '../', use path whitelisting. http://localhost:8082/xss_get.php/../../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 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/home Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/index Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/main Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/dashboard Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/admin Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/login Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/logout Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/profile Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/account Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/settings Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/config Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/users Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/api Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/api/users Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/api/admin Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/api/v1 Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/management Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/panel Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/control Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/search Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/help Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/about Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side.

http://localhost:8082/contact Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/register Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/signup Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/signin Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/forgot Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/reset Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/change-password Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/edit-profile Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/preferences Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/notifications Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/messages Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/inbox Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/reports Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/analytics Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/logs Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/admin/users Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/admin/settings Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/admin/reports Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/admin/logs Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user/profile Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user/settings Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user/dashboard Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/user/account Not Vulnerable Medium Rejected (HTTP 404) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/documents Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/images Vulnerable Medium Endpoint accepted POST (possible bypass) Restrict allowed HTTP methods, validate them server-side. http://localhost:8082/passwords 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/xss_get.php/admin Error Medium Request failed Enforce authentication/authorization on all sensitive endpoints. http://localhost:8082/xss_get.php/config Error Medium Request failed Enforce authentication/authorization on all sensitive endpoints. http://localhost:8082/xss_get.php/debug Error Medium Request failed Enforce authentication/authorization on all sensitive endpoints. http://localhost:8082/xss_get.php/private Error Medium Request failed Enforce authentication/authorization on all sensitive endpoints. Header/Token Tampering URL Status Risk Details Mitigation http://localhost:8082/xss_get.php/admin Error High Request failed Validate tokens strictly server-side; never trust missing or forged headers. http://localhost:8082/xss_get.php/config Error High Request failed Validate tokens strictly server-side; never trust missing or forged headers. http://localhost:8082/xss_get.php/private Error High Request failed Validate tokens strictly server-side; never trust missing or forged headers. Cookie Manipulation URL Status Risk Details Mitigation http://localhost:8082/xss_get.php/admin Error High Request failed Do not store roles in cookies; enforce all roles and permissions server-side. http://localhost:8082/xss_get.php/config Error High Request failed Do not store roles in cookies; enforce all roles and permissions server-side. CORS Misconfiguration URL Status Risk Details

Mitigation http://localhost:8082/xss_get.php Not Vulnerable Medium CORS restricted properly Restrict CORS Access-Control-Allow-Origin to trusted domains only. Unauthenticated Access URL Status Risk Details Mitigation - No endpoints evaluated Low No suitable URLs discovered or crawl empty General best practices