BAC Report - http://localhost:8082

BAC Report

BAC Report

Broken Access Control Report

Site: http://localhost:8082

Date: 2025-09-09_07-44-03

Note: Crawled 5 links successfully.Discovered links:http://localhost:8082/js/html5.jshttp://localhost:8082/user_new.phphttp://localhost:8082/info.phphttp://localhost:8082/training.phphttp://localhost:8082/login.php

Executive Summary This report details the Broken Access Control vulnerabilities identified on http://localhost:8082 during a security assessment conducted on 2025-09-09_07-44-03. A total of 10 tests were performed, resulting in 35 findings. Of these, 5 were identified as vulnerable, indicating potential weaknesses in the application's access control mechanisms. The most critical vulnerabilities include unauthorized access to administrative endpoints via Force Browsing, Header/Token Tampering, and Cookie Manipulation, as well as Method Bypass and Unauthenticated Access. Remediation steps for each vulnerability are outlined to improve the application's security posture. Summary Total Tests: 10 Total Findings: 35 Vulnerable: 5

Executive Summary

This report details the Broken Access Control vulnerabilities identified on http://localhost:8082 during a security assessment conducted on 2025-09-09_07-44-03. A total of 10 tests were performed, resulting in 35 findings. Of these, 5 were identified as vulnerable, indicating potential weaknesses in the application's access control mechanisms. The most critical vulnerabilities include unauthorized access to administrative endpoints via Force Browsing, Header/Token Tampering, and Cookie Manipulation, as well as Method Bypass and Unauthenticated Access. Remediation steps for each vulnerability are outlined to improve the application's security posture.

Summary

Total Tests: 10

Total Findings: 35

Vulnerable: 5

IDOR

Path IDOR

Privilege Escalation

Directory Traversal

Method Bypass

Force Browsing

Header/Token Tampering

Cookie Manipulation

CORS Misconfiguration

Unauthenticated Access