BAC Report - http://localhost:8082

bac_report

bac_report

Broken Access Control Report

Site: http://localhost:8082

Date: 2025-09-09_02-09-46

Note: Crawled 19 links successfully.Discovered links:http://localhost:8082/info.phphttp://localhost:8082/images/mme.pnghttp://localhost:8082/images/facebook.pnghttp://localhost:8082/images/blogger.pnghttp://localhost:8082/images/netsparker.pnghttp://localhost:8082/images/favicon.icohttp://localhost:8082/images/mk.pnghttp://localhost:8082/images/twitter.pnghttp://localhost:8082/images/netsparker.gifhttp://localhost:8082/images/bee_1.pnghttp://localhost:8082/images/zap.pnghttp://localhost:8082/user_new.phphttp://localhost:8082/training.phphttp://localhost:8082/login.phphttp://localhost:8082/stylesheets/stylesheet.csshttp://localhost:8082/images/cc.pnghttp://localhost:8082/js/html5.jshttp://localhost:8082/images/owasp.pnghttp://localhost:8082/images/linkedin.png

Executive Summary This report details the findings of a Broken Access Control (BAC) assessment performed on http://localhost:8082 on 2025-09-09_02-09-46. The assessment aimed to identify vulnerabilities related to unauthorized access to resources and functionalities. A total of 10 tests were conducted, resulting in 85 findings. Of these, 29 were identified as vulnerable. Key vulnerabilities identified include Method Bypass, Force Browsing, Header/Token Tampering, Cookie Manipulation, and Unauthenticated Access. Recommendations are provided for each vulnerability type to remediate these issues and improve the overall security posture of the application. Summary Total Tests: 10 Total Findings: 85 Vulnerable: 29

Executive Summary

This report details the findings of a Broken Access Control (BAC) assessment performed on http://localhost:8082 on 2025-09-09_02-09-46. The assessment aimed to identify vulnerabilities related to unauthorized access to resources and functionalities. A total of 10 tests were conducted, resulting in 85 findings. Of these, 29 were identified as vulnerable.

Key vulnerabilities identified include Method Bypass, Force Browsing, Header/Token Tampering, Cookie Manipulation, and Unauthenticated Access. Recommendations are provided for each vulnerability type to remediate these issues and improve the overall security posture of the application.

Summary

Total Tests: 10

Total Findings: 85

Vulnerable: 29

IDOR

Path IDOR

Privilege Escalation

Directory Traversal

Method Bypass

Force Browsing

Header/Token Tampering

Cookie Manipulation

CORS Misconfiguration

Unauthenticated Access