VULNERABILITY ASSESSMENT REPORT

FUTURE-CS-01

Scope and Ethics

SCOPE OF ASSESSMENT

- PUBLIC FACING PAGES ONLY
- READ-ONLY ANALYSIS
- NO LOGIN, NO EXPLOITATION

TOOLS USED

- BROWSER DEVELOPER TOOLS

FINDING - 1 [MISSING SECURITY HEADER]

DESCRIPTION

- THE WEBSITE DOES NOT IMPLEMENT IMPORTANT HTTP SECURITY HEADERS SUCH AS CONTENT-SECURITY-POLICY AND X-FRAME-OPTIONS.

WHY IT MATTERS

- MISSING SECURITY HEADERS CAN EXPOSE USERS TO CLICKJACKING AND MALICIOUS SCRIPT INJECTION ATTACKS

RISK LEVEL - MEDIUM

RECOMENDED FIX - CONFIGURE THE WEB SERVER TO INCLUDE STANDARD HTTP SECURITY HEADERS.

FINDING - 2 [Server Information Disclosure]

DESCRIPTION

- HTTP RESPONSE HEADERS REVEAL SERVER AND TECHNOLOGY INFORMATION.

WHY IT MATTERS

- EXPOSED SERVER DETAILS CAN HELP ATTACKERS UNDERSTAND BACKEND TECHNOLOGIES.

RISK LEVEL - LOW

RECOMENDED FIX - REMOVE OR HIDE UNNECESSARY SERVER-RELATED HEADERS.

FINDING - 3 [No HTTPS Enforcement]

DESCRIPTION

- THE WEBSITE IS ACCESSIBLE OVER HTTP WITHOUT ENFORCING HTTPS.

WHY IT MATTERS

- UNENCRYPTED COMMUNICATION CAN BE INTERCEPTED OR MODIFIED.

RISK LEVEL - HIGH

RECOMENDED FIX - IMPLEMENT HTTPS AND REDIRECT ALL HTTP TRAFFIC TO HTTPS.

CONCLUSION

THIS ASSESSMENT IDENTIFIED COMMON CONFIGURATION-LEVEL SECURITY ISSUES USING PASSIVE BROWSER-BASED ANALYSIS. NO EXPLOITATION OR AGGRESSIVE TESTING WAS PERFORMED. ALL FINDINGS CAN BE RESOLVED USING STANDARD SECURITY BEST PRACTICES