AUDACIX | CYBER CHIEF
Powered By Audacix

CERTIFICATE OF APPLICATION SECURITY

After conducting thorough and exhaustive security testing on the CoachingLoft web application, APIs and network infrastructure in accordance with OWASP's ASVS Level 2, we confirm that zero known high or medium risk security vulnerabilities are unpatched as at 20 December 2021.

We can also confirm that the company has implemented exhaustive vulnerability scanning processes to find and fix vulnerabilities that may arise in the future.

Tests for the following application security vulnerabilities were conducted by our OSCP/CEH accredited penetration testers:

Application

Unused HTTP Methods available
Missing Input Validation
Application Errors
Unprotected Admin Pages
Malicious File Upload
Open Mail Service
Insecure File Upload
Missing Function Level Access Control
Unauthorized URL Access
Source Code disclosure
Test, Sample, Debug, Monitoring Pages Available
Frameable Response
Unprotected Open Services
Data Manipulation With GET Requests
IP Restriction Bypass Possible
Missing or Insufficient Security Configuration
Resource Enumeration
External Libraries Without Integrity Check
Unauthorized Unencrypted Data Access
Unvalidated Redirect
HTML Response Found In Redirect

Information Disclosure

Improper Error Handling
Unmasked Sensitive Data
Directory Listings Available
Sensitive Data in Logs
Disclosure of Credentials
Sensitive Data in URL Parameters
Software Components Disclosure
Technical Information Disclosure
Software Components Disclosure
Web Directory Enumeration
Open Directory Listings
Comments in HTML Sources
Output of Application Stacktraces
Internal Servername

Infrastructure

Old/Vulnerable Software
Operating System Versions
Bypassing Firewall Rules
Filtered Port Recognition
Open Services/Ports
Missing SPF Header

Session Handling

Improper Session Logout
Insecure Session Cookie
Insecure Cookie State Changes
Persistent Session Cookie
Session Cookie Guessable or Random
Improper Session Timeouts
Session Cookie Data Disclosure
Session Fixation
Session Cookie Not HttpOnly

Encryption

Authentication Credentials Without Encryption
Weak SSL/TLS Configuration
Payload/Data Without Transport Encryption
Certificate Errors/Warnings
Weak Password Hash Algorithm
No HTTP Strict Transport Security
Insecure SSL/TLS
Secure Pages With Mixed Content

Injections

Dynamic HTML Injection
Filename Injection
Static HTML Injection
Cross Site Request Forgery
Database, Directory Injection
Server Side Request Forgery
Blind Database, Direcoty Injection
Code Injection
Flash Configuration

Authentication

Weak Password Policy
Authentication Bypass
Password Auto-Complete
Takeover
Weak Forgot Password Feature
Weak Captcha
Improper Account Locking
Missing Security Approvals
Plain Password Sent To User
Username Brute Forceable
Privilege Escalation
Credentials brute-force able
Authentication Backdoor
Weak User Accounts & IDs
Password Field Response

Ayush Trivedi

Digitally signed by A Trivedi
Date: 2021.12.23 13:54:47 +11'00'

Approving Director