Web Application Penetration Testing Report

Prepared by:
Md. Nazmur Sakib(nazmursakib30@gmail.com)
Intern
Department: Technology Governance & Cyber Security Management
Banglalink Digital Communication Limited

Prepared for: Banglalink Digital Communication Limited

Reviewed by:
Md Shahriar Hussain(shahriar.hussain@banglalink.net)
Cyber Security & Compliance Lead Engineer
Department: Technology Governance & Cyber Security Management
Banglalink Digital Communication Limited

Limitation of disclosure and use of the document:

This report was prepared for the comprehensive study of web application penetration testing. This report contains information about potential vulnerabilities of the www.banglalink.net web application. The document gives no warranties concerning 100% accuracy, reliability, quality, correctness, or freedom from error or omission of this work. This report is delivered "as is", it shall not be liable for any inaccuracy in any condition. This paper also does not assure any form of warranty or guarantee that the system is 100% secure from security attacks that are not mentioned in the report.

Document Details:

Title: Web Application(Black Box) Penetration testing.
Project name: www.banglalink.net
Project Duration: 19/01/2021 - /02/2022

Contents

Executive Summary:

The primary purpose of this web application (Black box) penetration testing was to determine any possible areas of concern associated with the web application and identify to which extent the system can be exploited by an attacker possessing a particular skill and motivation. This web application penetration testing was performed following the Open Web Application Security Project (OWASP) guideline. The penetration testing was conducted from January 19 to February 16, 2020. All testing activities were conducted as an external attacker without prior knowledge of the environment and were completely isolated from the production data.

During the course of this assessment, no critical vulnerabilities were found that could lead to complete compromise of the system. Nevertheless, some medium and low severity issues were found, which should be addressed. Though any high-security flaws were not found, it is recommended to remediate all medium-security issues detected to mitigate against the possible risk of a sensitive data compromise. The remediation of the low severity findings is not so urgent due to the low probability of their successful exploitation. However, the presence of these known issues could decrease the system's overall security.

The scope of the assessment included the following:

https://www.banglalink.net/ (business-critical corporate Web Application with multiple features)

Testing was performed using industry-standard penetration testing tools and frameworks, including Nmap,Acunetix, DirBuster, Wireshark, OWASP ZAP and Burp Suite.

WEB APPLICATION RESULTS:

Vulnerability Result	
Vulnerabilities Found	YES
Exploited – Denial of Service (DoS)	NO
Exploited – Elevation of Privilege (EoP)	NO
Exploited – Remote Code Execution (RCE)	NO
Exploit Persistence Achieved	NO
Sensitive Data Exfiltrated	NO
Overall Risk	Medium

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

OWASP 2021 Top 10	Number of Alerts
A01: Broken Access Control	1 Alarts
A02: Cryptographic Failures	5 Alerts
A03: Injection	N/A
A04: Insecure Design	N/A
A05: Security Misconfiguration	3 Alarts
A06: Vulnerable and Outdated Components	3 Alarts
A07: Identification and Authentication Failures	N/A
A08: Software and Data Integrity Failures	N/A
A09: Security Logging and Monitoring Failures	N/A
A10: Server-Side Request Forgery	N/A

Automated Application scan and crawling:

Several commercial tools were used to scan the targeted scope and identify potential vulnerabilities. The automated scanning software identifies application-level vulnerabilities. The web application crawling covered the following:

- Parameter Injection
- SQL Injection
- Cross-Site Scripting
- Directory Traversal
- Parameter Overflow
- Buffer Overflow
- Parameter Addition
- Path Manipulation
- Character Encoding
- Site Search
- SSL Strength
- Sensitive Developer Comments
- Web Server Identification
- Web Package Identification
- Permissions Assessment
- Brute Force Authentication attacks

Manual Application Testing:
Using the information created by the automated testing software, some manual testing was done to identify and exploit additional vulnerabilities in the targeted application and eliminate false positives produced by the automatic scanning methods.

Following actions were performed as part of manual testing:

- The gathered information about the application
- Checked types and placement of security controls
- Mapped application content and analyzed it
- Tested application authentication, session management and access control
- Tested application for input based vulnerabilities
- Tested application for client data validation issues
- Checked for application server vulnerabilities
- Tested HTTP/URL manipulation
- Tested SQL command injection
- Tested cross-site scripting
- Tested Cross-site request forgery
- Tested DOS attacks
- Tested Parameter overflow and handling

- Checked Information leakage
- Checked outdated plugins

Web Application Detailed vulnerabilities Findings:

A01: Broken Access Control: