

Mobile Application Penetration Testing Report (MyBL)

Prepared by:

Technology Governance & Cyber Security Management Department
Banglalink Digital Communication Limited

Prepared for:

Banglalink Digital Communication Limited

March, 2022

Limitation of disclosure and use of the document:

This report contains information about potential vulnerabilities of the MyBL (My Banglalink)) mobile 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: Mobile Application(Black Box) Penetration testing.

Application Name: MyBL (My Banglalink)

Application Type: Android

Package Name: com.arena.banglalinkmela.app

Application Version: 9.0.0.3

Project Duration: 20/02/2021 - 15/03/2022

Contents

1	EXECUTIVE SUMMARY:	1
2	Mobile APPLICATION VULNERABILITIES RESULTS:	3
3	SCANNING AND TESTING	6
3.1	Automated Application scan and crawling:	6
3.2	Manual Application Testing:	7
4	Web Application Detailed vulnerabilities Findings:	10
4.1	User authentication Using the Bruteforce method:	11
4.2	Content management admin login panel accessible via public IP. . .	12
4.3	Insecure 1024-bit RSA Signing-key.	14
4.4	Weak Password Policy for User Accounts.	16
4.5	Certificates signed by non-trusted are accepted.	17
4.6	Backdated Apache Server	18
4.7	Application has set insecure Permissions.	19
4.8	Use of the weak encryption mode CBC with PKCS5/PKCS7 padding. .	20

4.9	Information considered sensitive in the context of security of the mobile app is identified.	22
4.10	The application can be installed and run after reverse engineered. .	24
4.11	The app does not inform the user of all sensitive activities with their account.	26
4.12	Use of Insufficiently Random Values.	26
4.13	No security against rooted or jailbroken devices	27
4.14	The app does not prevent debugging and/or detects and responds when a debugger is attached.	29
5	Conculation	31

1. EXECUTIVE SUMMARY:

The primary purpose of this mobile application (Black box) penetration testing was to determine any possible areas of concern associated with the mobile 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 The OWASP Mobile Application Security Verification Standard (MASVS v1.4.2) and The OWASP Mobile Security Testing Guide (MSTG v1.4.0). The penetration testing was conducted from February 20 to March 10, 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, some critical vulnerabilities were found that could lead to serious damage to the system. Along with that, some medium and low severity issues were found, which should be addressed. As some high-security flaws were found, it is recommended to remediate all high-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:

Components and interfaces of [My BL\(My Banglalink\)](#) android application.

Testing was performed using industry-standard penetration testing tools and frameworks. Including, Burp Suite, OWASP ZAP, Drozer, ADB, PID Cat and MobSF.

2. Mobile APPLICATION VULNERABILITIES RESULTS:

OWASP MSTG and MASTVS:

The OWASP Mobile Security Testing Guide is an OWASP flagship project led by Carlos Holguera and Sven Schleier which defines the industry standard for mobile application security.

<https://owasp.org/www-project-mobile-security-testing-guide/>

The OWASP MASVS (Mobile Application Security Verification Standard) is a standard that establishes the security requirements for mobile app security.

<https://github.com/OWASP/owasp-mstg/>

ID	Risk Category	Number of Alerts
MSTG-1	Architecture, Design and Threat Modeling	1 Alerts
MSTG-2	Data Storage and Privacy	N/A
MSTG-3	Cryptography	2 Alerts
MSTG-4	Authentication and Session Management	3 Alerts
MSTG-5	Network Communication	2 Alerts
MSTG-6	Platform Interaction	2 Alerts
MSTG-7	Code Quality and Build	1 Alerts
MSTG-8	Resilience	4 Alerts
	Total =	15

Figure 2.1: Checklist Using OWASP MSTG v1.4.0 and MASTVS v1.4.2

ID	MSTG-ID	Findings	L1	L2	R	Risk
4.6	MSTG-AUTH-6	Able to authenticate on the application Using the Bruteforce method.	✓			High
6.3	MSTG-PLATFORM-3	CMS admin login panel of this application is accessible via public IP.	✓			High
1.4	MSTG-ARCH-4	Information considered sensitive in the context of security of the mobile app is identified.		✓		Mid
3.4	MSTG-CRYPTO-4	The app uses the weak encryption mode CBC with PKCS5/PKCS7 padding.		✓		Mid
4.5	MSTG-AUTH-5	Weak password policy for user accounts.		✓		Mid
5.4	MSTG-NETWORK-4	Certificates signed by non-trusted are accepted.		✓		Mid
5.6	MSTG-NETWORK-6	The app runs on backdated Apache server version 2.4.29, which is venerable to different attacks.		✓		Mid
6.1	MSTG-PLATFORM-1	Application has set insecure Permissions.		✓		Mid
7.1	MSTG-CODE-1	The application uses a1024-bit RSA Signing-key, which is considered a security risk.		✓		Mid
8.4	MSTG-RESILIENCE-4	The application can be installed and run after reverse engineered.			✓	Mid
3.6	MSTG-CRYPTO-6	Use of Insufficiently Random Values.		✓		Low
4.11	MSTG-AUTH-11	The app does not inform the user of all sensitive activities with their account. There is no feature for users to view the list of devices, view contextual information (IP address, location, etc.), and block specific devices.		✓		low
8.1	MSTG-RESILIENCE-1	The app does not detect and responds to the presence of a rooted or jailbroken device either by alerting the user or terminating the app.			✓	Low
8.2	MSTG-RESILIENCE-2	The app does not prevent debugging and/or detects and responds when a debugger is attached.			✓	Low
8.5	MSTG-RESILIENCE-5	The app does not detect and respond to being run in an emulator.			✓	Low
Overall Risk = High						

Figure 2.2: Summary of Vulnerabilities Found

3. SCANNING AND TESTING

3.1 Automated Application scan and crawling:

Several commercial tools were used to scan the targeted application and identify potential vulnerabilities. The automated scanning software identifies application-level vulnerabilities. The automatic 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

3.2 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
- Checked Brute Force Authentication
- Tested Reverse Engineering
- Checked Application Signature

-
- Tested Application Permission
 - Checked Cached Files
 - Checked injection
 - Checked Accessible Content URIs
 - Checked Path Traversal
 - Tested Application Signing
 - Tested DOS attacks
 - Checked Hidden Folders

OWASP Risk Assessment Calculator

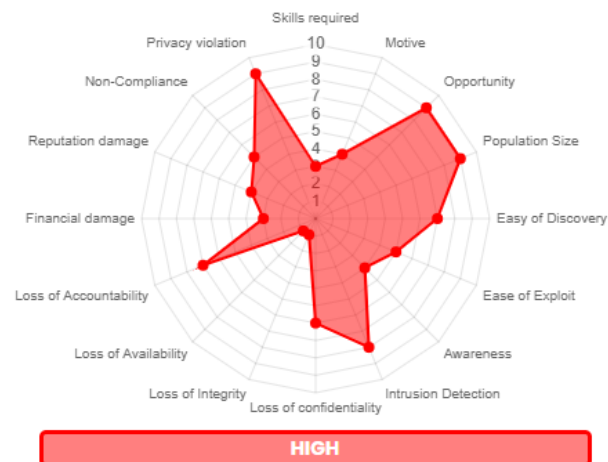


Figure 3.1: OWASP Risk Assessment

4. Web Application Detailed vulnerabilities Findings:

4.1 User authentication Using the Brute force method:

Classification: High Risk

CWE ID: CWE-307

Improper Restriction of Excessive Authentication Attempts.

OWASP MSTG-ID: MSTG-AUTH-6

Description:

The software does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame for password-based login, making it susceptible to brute force attacks. The application allowed multiple authentication requests when tested against a brute force cluster bomb attack using Burp Suite intruder. As the number is fixed for a particular user, that makes it very easy for an attacker to use regex in the password and perform a successful brute force attack.

Solution:

Solution: An IP address should be blocked for a time span for password-based login after 3 to 5 failed authentication attempts. It is recommended that for the time being, only OTP-based login should be enabled before fixing the password-based login system.

38	Mns78931.	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
39	Mns78933.	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
40	Mns78932.	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
41	aghahs1234	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	631
42	12123asdf	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
43	www1234	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
44	Mns78931	01404400712	200	<input type="checkbox"/>	<input type="checkbox"/>	2876
45	5654absa	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
46	yety5656	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
47	treyeq456	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611
48	gfgfs5657	01404400712	401	<input type="checkbox"/>	<input type="checkbox"/>	611

Request	Response
Raw	Headers Hex

```

HTTP/1.1 200 OK
Date: Tue, 01 Mar 2022 05:30:03 GMT
Server: Apache/2.4.41 (Unix)
X-Powered-By: PHP/7.3.11
Cache-Control: no-cache, private
Access-Control-Allow-Origin: https://mybl.banglalinkr.net
Access-Control-Allow-Headers: X-PINGOTHER, Content-Type, authorization, api-client-pass, pl
Access-Control-Allow-Methods: POST, GET, OPTIONS
Keep-Alive: timeout=5, max=73
Connection: Keep-Alive
Content-Type: application/json
Content-Length: 2399

{"status": "SUCCESS", "status_code": 200, "message": "Login
Successfully", "data": {"token": {"token_type": "Bearer", "expires_in": 31536000, "access_token": "s

```

Figure 4.1: login using brute force

4.2 Content management admin login panel accessible via public IP.

Classification: High Risk

CWE ID: 284

Improper Access Control

OWASP MSTG-ID: MSTG-PLATFORM-3

Description:

This application's content management system admin panel is accessible via any

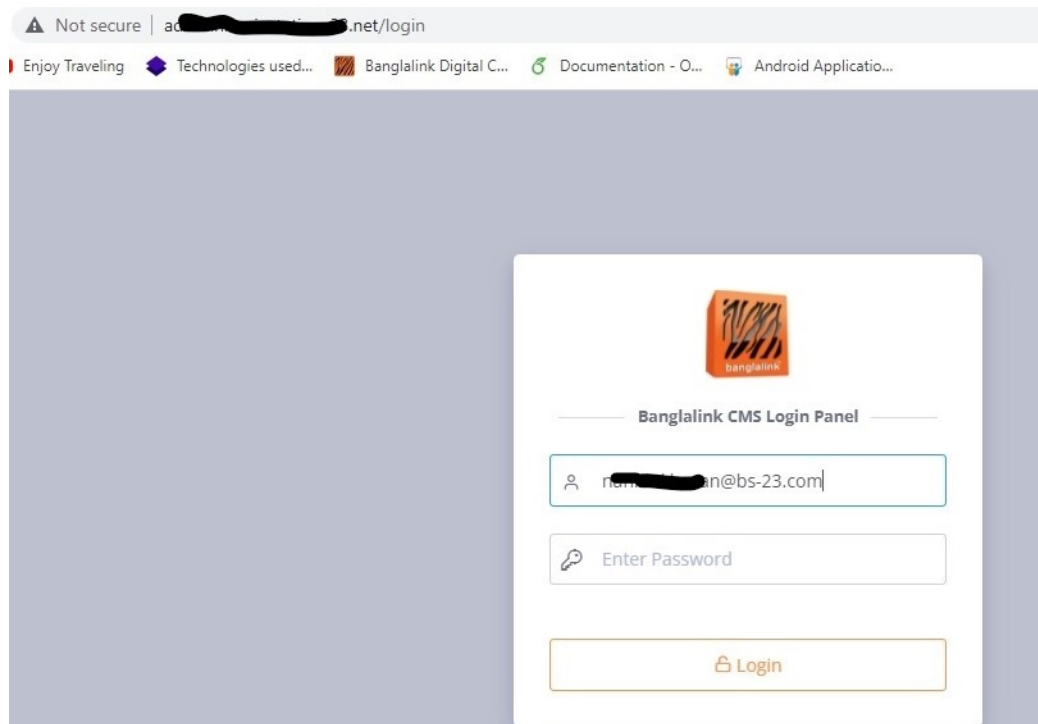


Figure 4.2: CMS Admin Login panel

public IP address. If we dig further, it reveals some sensitive information that might help a remote attacker break into the admin panel of the CMS of this Application. So the site does not use a secure transmission protocol.

Solution:

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Server/Request Data	
REDIRECT_STATUS	"200"
HTTP_HOST	"admin.brainstation-23.net"
HTTP_X_FORWARDED_SCHEME	"http"
HTTP_X_FORWARDED_PROTO	"http"
HTTP_X_FORWARDED_FOR	"103.67.158.163"
HTTP_X_REAL_IP	"103.67.158.163"
HTTP_CONNECTION	"close"
CONTENT_LENGTH	"88"

3/2/22, 10:44 AM	Whoops! There was an error.
HTTP_CACHE_CONTROL	"max-age=0"
HTTP_UPGRADE_INSECURE_REQUESTS	"1"
HTTP_ORIGIN	"http://admin.brainstation-23.net"
CONTENT_TYPE	"application/x-www-form-urlencoded"
HTTP_USER_AGENT	"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
HTTP_ACCEPT	"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
HTTP_REFERER	"http://admin.brainstation-23.net/login"
HTTP_ACCEPT_ENCODING	"gzip, deflate"
HTTP_ACCEPT_LANGUAGE	"en-US,en;q=0.9"
HTTP_COOKIE	"XSRF-TOKEN=eyJpdii6I1JNqlwOUx50GRjQmLFNTRQqXBHlWvQT09IiwidmFsdWUiOiJ
PATH	"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
SERVER_SIGNATURE	"<address>Apache/2.4.29 (Ubuntu) Server at admin.brainstation-23.net P
SERVER_SOFTWARE	"Apache/2.4.29 (Ubuntu)"
SERVER_NAME	"admin.brainstation-23.net"
SERVER_ADDR	"192.168.104.238"
SERVER_PORT	"80"
REMOTE_ADDR	"172.16.229.109"
DOCUMENT_ROOT	"/var/www/html/bl_cms/public"
REQUEST_SCHEME	"http"
CONTEXT_PREFIX	""
CONTEXT_DOCUMENT_ROOT	"/var/www/html/bl_cms/public"
SERVER_ADMIN	"[REDACTED]@bs-23.com"

Figure 4.3: CMS Admin panel information

4.3 Insecure 1024-bit RSA Signing-key.

Classification: Medium Risk

CWE ID: 327

Use of a Broken or Risky Cryptographic Algorithm

OWASP MSTG-ID: MSTG-CODE-1

```

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=BD, ST=dhaka, L=dhaka, O=banglalink, OU=banglalink, CN=banglalink
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-02-25 15:27:42+00:00
Valid To: 2039-02-19 15:27:42+00:00
Issuer: C=BD, ST=dhaka, L=dhaka, O=banglalink, OU=banglalink, CN=banglalink
Serial Number: 0x530cb66e
Hash Algorithm: sha1
md5: deb75dad27cf4da195559333c3aab0c1
sha1: eb748a82d4398c4df6962f7380988ea9d4e073dc
sha256: a1a6d472561dae3b8816cb36f4dbe560b601a847288aa4e926093110ca3ffed9
sha512: 1b252f8f10364c37b735ce8bdce394a82fb5d7be125e799b1dd844114980532b36dfec4aa7213d5
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 21188bafd3bcad0e1ec04f2fc5467f444dbec47c26093a7309388fd6b0d66a8e|
Is CN=banglalink, OU=banglalink, O=banglalink, L=dhaka, ST=dhaka, C=BD correct?
[no]: yes
Generating 1,024 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 2,542 days
for: CN=banglalink, OU=banglalink, O=banglalink, L=dhaka, ST=dhaka, C=BD
Warning:
The generated certificate uses a 1024-bit RSA key which is considered a security risk. This key size will be disabled in a future update.

```

Figure 4.4: Application digital signature

Description:

The application uses a 1024-bit RSA Signing-key according to MobsF, which is no longer considered as a secure key for application certificate signing. The use of a non-standard algorithm is dangerous because a determined attacker may break the algorithm and compromise whatever data has been protected.



Solution:

Solution: The application's digital signature key should be updated with a more secure signing algorithm.

Change Password

Password must be minimum 8 characters and contain at least one letter and one number

Old Password

••••••••  


 Password must be minimum 8 characters and contain at least one letter and one number

Figure 4.5: Password Policy of MyBL

4.4 Weak Password Policy for User Accounts.

Classification: Medium Risk

CWE ID: 521

Weak Password Requirements

OWASP MSTG-ID: MSTG-AUTH-5

Description:

This application does not require that users have strong passwords, making it easier for attackers to compromise user accounts. Therefore, this password must be of sufficient complexity and impractical for an adversary to guess. Selecting the correct password requirements and enforcing them through implementation are critical to the overall success of the authentication mechanism. The user account password in this application is not mandatory to use upper case, lower case or special characters, making it easy for brute force attacks.

Solution:

Password should contain lower case, upper case alphabet, special character, along with the current policy to make it stronger.

4.5 Certificates signed by non-trusted are accepted.

Classification: Medium Risk

CWE ID: 295

Improper Certificate Validation

OWASP MSTG-ID: MSTG-AUTH-5

Description:

While reverse-engineering the software, the application accepted and worked with the digital signing certificate provided.

Solution:

There should be a mechanism to prevent application certificates signed from non

```
>>> Signer
X.509, CN=banglalink, OU=banglalink, O=banglalink, L=dhaka, ST=dhaka, C=BD
Signature algorithm: SHA256withRSA, 1024-bit key (weak)
[trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
The RSA signing key has a keysize of 1024 which is considered a security risk. This key size will be disabled in a future update.
D:\Pen_Testing Tool\Reverse eng apk\dex-tools-2.1\mybl\dist>
```

Figure 4.6: Signing MyBL App

trusted, or there should be some warning for non-trusted certificated applications during installation.

4.6 Backdated Apache Server

Classification: Medium Risk

CWE ID: 672

Operation on a Resource after Expiration or Release

OWASP MSTG-ID: MSTG-AUTH-5

Description:

During reconnaissance, it was found that the application is using an out-of-date version of Apache, which is v-2.4.29, and this version has multiple vulnerabilities.

Solution:

It is recommended to upgrade the Apache version to the latest.

```
HTTP_COOKIE      "XSRF-TOKEN=eyJpdii6I1JNqlwvOUx5OGRjQm1FNTRQXXBHU1wvQT09IiwidmFsdWUiOiJ  
PATH             "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin  
SERVER_SIGNATURE "<address>Apache/2.4.29 (Ubuntu) Server at admin.brainstation-23.net P  
SERVER_SOFTWARE  "Apache/2.4.29 (Ubuntu)"
```

Figure 4.7: Apache Version

Apache » Http Server » 2.4.29 * * * : Security Vulnerabilities

Cpe Name: cpe:2.3:a:apache:http_server:2.4.29:*:*:*:*:*:*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-17189 400				2019-01-30	2021-07-06	5.0	None	Remote	Low	Not required	None	None	Partial

In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

2	CVE-2017-15710 787			DoS	2018-03-26	2021-06-06	5.0	None	Remote	Low	Not required	None	None	Partial
---	----------------------------------------------------	--	--	-----	------------	------------	-----	------	--------	-----	--------------	------	------	---------

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

Figure 4.8: vulnerabilities of Apache Version 2.4.29

4.7 Application has set insecure Permissions.

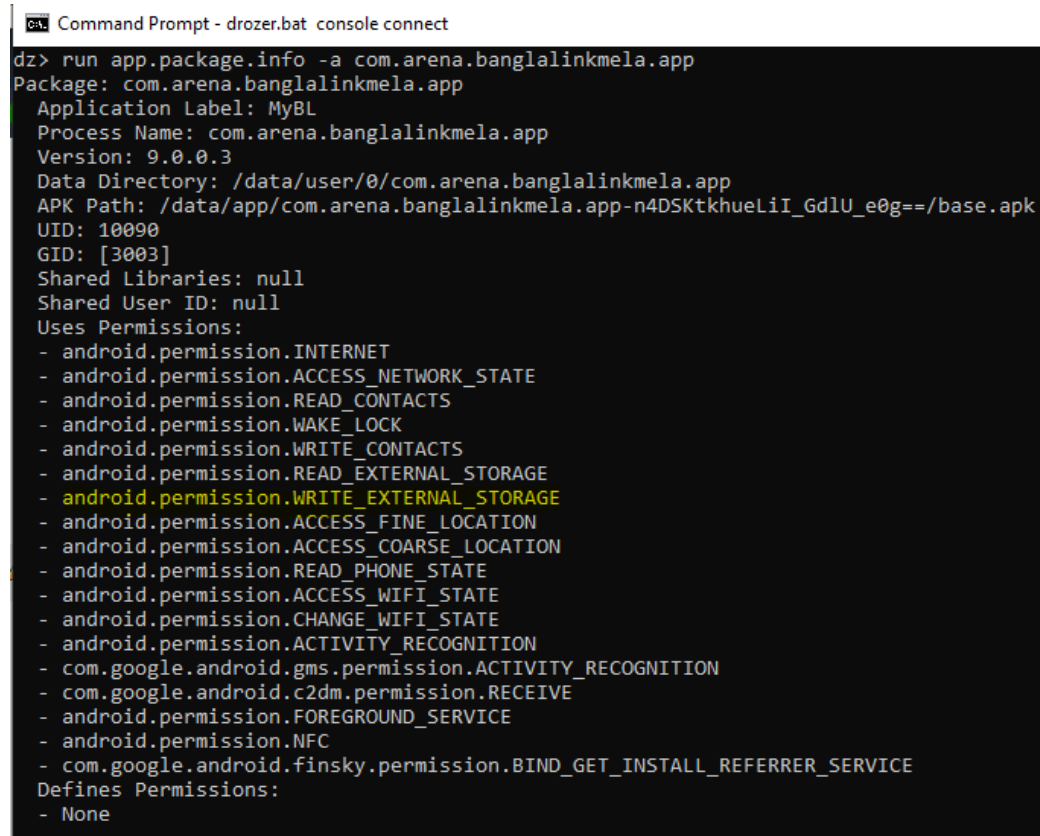
Classification: Medium Risk**CWE ID:** 250

Execution with Unnecessary Privileges

OWASP MSTG-ID: MSTG-PLATFORM-1**Description:**

Permission mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad hoc access to specific pieces of data. It was observed that application has set insecure permissions, which will create security threat to an application.

Solution:



```

C:\> Command Prompt - drozer.bat console connect
dz> run app.package.info -a com.arena.banglalinkmela.app
Package: com.arena.banglalinkmela.app
Application Label: MyBL
Process Name: com.arena.banglalinkmela.app
Version: 9.0.0.3
Data Directory: /data/user/0/com.arena.banglalinkmela.app
APK Path: /data/app/com.arena.banglalinkmela.app-n4DSKtkhueLiI_GdIU_e0g==/base.apk
UID: 10090
GID: [3003]
Shared Libraries: null
Shared User ID: null
Uses Permissions:
- android.permission.INTERNET
- android.permission.ACCESS_NETWORK_STATE
- android.permission.READ_CONTACTS
- android.permission.WAKE_LOCK
- android.permission.WRITE_CONTACTS
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_FINE_LOCATION
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.READ_PHONE_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.CHANGE_WIFI_STATE
- android.permission.ACTIVITY_RECOGNITION
- com.google.android.gms.permission.ACTIVITY_RECOGNITION
- com.google.android.c2dm.permission.RECEIVE
- android.permission.FOREGROUND_SERVICE
- android.permission.NFC
- com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
Defines Permissions:
- None

```

Figure 4.9: MyBL Application Permissions

Implement or set only necessary permissions for your application.

4.8 Use of the weak encryption mode CBC with PKCS5/PKCS7 padding.

Classification: Medium Risk

CWE ID: 649

Reliance on Obfuscation or Encryption of Security-Relevant Inputs without In-

egrity Checking

OWASP MSTG-ID: MSTG-CRYPTO-4

Description:

The application uses encryption mode CBC with weak PKCS5/PKCS7 padding for SSLwireless transaction API, which is vulnerable to Padding Oracle Attacks due to Weaker Padding or Block Operation Implementations may affect the user state, system state, or some decision made on the server. Without protecting the tokens/parameters for integrity, the application is vulnerable to an attack where an adversary traverses the space of possible values of the said token/parameter to attempt to gain an advantage. The attacker's goal is to find another admissible value that will somehow elevate their privileges in the system, disclose information, or change the system's behaviour in some way beneficial to the attacker. If the application does not protect these critical tokens/parameters for integrity, it will not be able to determine that these values have been tampered with. Measures that are used to protect data for confidentiality should not be relied upon to provide the integrity service.

Solution:

To protect against padding oracles, you want to ensure that your application does not return a different error when the padding is wrong. The best way to do this is an Encrypt-then-MAC construction, where a Message Authentication Code (MAC) is applied to the ciphertext. If the MAC fails, you don't need to look at the padding. If the MAC is correct, it is cryptographically unlikely that the padding has been

NO ↕	ISSUE ↕	SEVERITY ↕	STANDARDS ↕	FILES
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security- Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG- CRYPTO-3	com/sslwireless/sslcommerzlibrary/model/util/SSLSecurePrefs.java d/h/a/b/g1/g0/d.java

Figure 4.10: MobSF Scan Result

tampered with.

4.9 Information considered sensitive in the context of security of the mobile app is identified.

Classification: Medium Risk

CWE ID: 319

Cleartext Transmission of Sensitive Information

OWASP MSTG-ID: MSTG-ARCH-4

Description:

The software transmits sensitive or security-critical data in clear text in a commu-

NO ↑↓	SCOPE ↑↓	SEVERITY ↑↓	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	myblapi.brainstation-23.net admin.brainstation-23.net myblapi.banglalink.net 203.223.93.172 203.223.93.176 clients3.google.com 172.217.163.206	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

Figure 4.11: MobSF Scan Result

nication channel that can be sniffed by unauthorized actors and exposes sensitive information to an actor who is not explicitly authorized to access that information. Domain config is insecurely configured to permit cleartext traffic to these domains in scope.

Solution:

Domain config should be securely configured, and applications should hide all sensitive communications between the client and the server.

4.10 The application can be installed and run after reverse engineered.

Classification: Medium Risk

CWE ID: 829

Inclusion of Functionality from Untrusted Control Sphere

OWASP MSTG-ID: MSTG-RESILIENCE-4

Description:

The application can easily be reverse-engineered and runs without any issue after reverse engineering. Also, this app connects to its server and responds on the reverse-engineered app.

Solution:

Though it is impossible to prevent the Android app from reverse engineering, some necessary protocols should be implemented so that reverse-engineered apps don't run after connecting to the server.

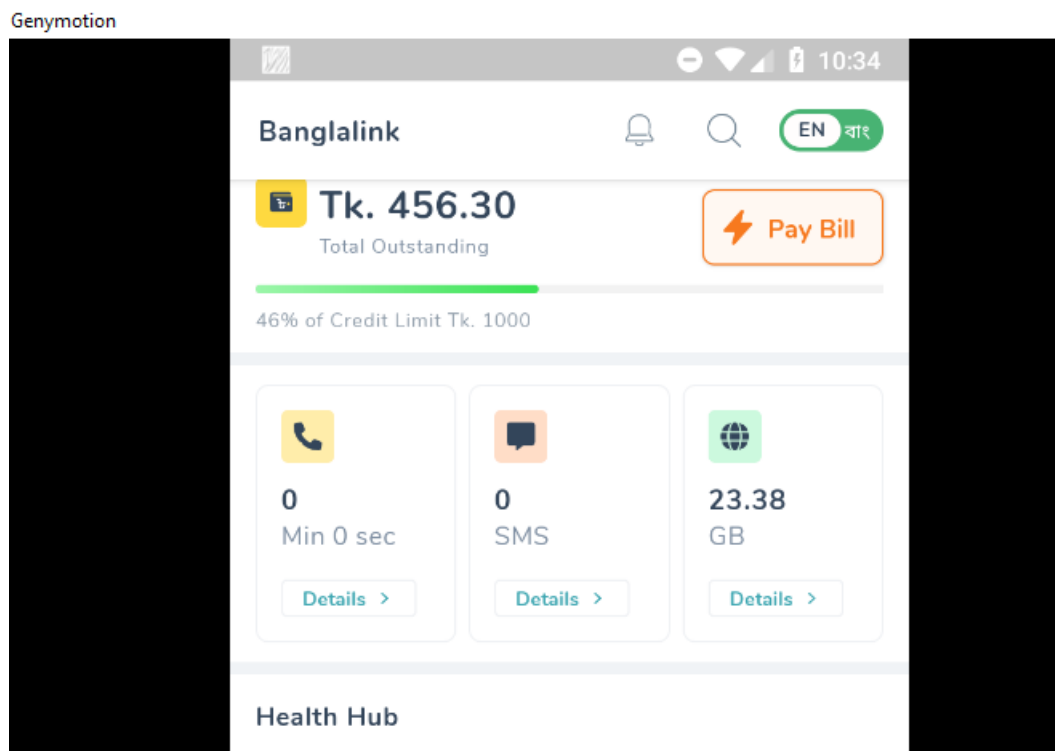


Figure 4.12: Reverse-engineered MyBL Application

4.11 The app does not inform the user of all sensitive activities with their account.

Incorrect Permission Assignment for Critical Resource

OWASP MSTG-ID: MSTG-AUTH-11

Description:

There is no feature for users to view the list of devices, view contextual information (IP address, location, etc.), and block specific devices. There are no alert messages or notifications set when someone logIn using the password authentication. So if an attacker breaks into someone else accounts, the user won't have any knowledge of that suspicious activity.

Solution:

There should be features for users to view the list of devices, view contextual information (IP address, location, etc.), and actions like block specific devices.

4.12 Use of Insufficiently Random Values.

Classification: Low Risk

CWE ID: 300

Use of Insufficiently Random Values

OWASP MSTG-ID: MSTG-CRYPTO-6

Description:


The App uses an insecure Random Number Generator.		CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/medallia/digital/mobilesdk/k5.java d/h/a/d/k/b/t9.java k/a/e2/a.java j/w/a.java d/h/a/d/h/m/h0.java d/h/a/d/h/c/b.java j/w/b.java com/sslwireless/sslcommerzlibrary/model/util/SSLShareInfo.java
-------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 4.13: MobSF Scan Result

The software uses insufficiently random numbers or values in a security context that depends on unpredictable numbers.

Solution:

Secure random numbers should be generated.

4.13 No security against rooted or jailbroken devices

Classification: Low Risk

OWASP MSTG-ID: MSTG-RESILIENCE-1, MSTG-RESILIENCE-5 .

Description:

The app does not detect and do not responds to the presence of a rooted or jailbroken device either by alerting the user or terminating the app. This application ran

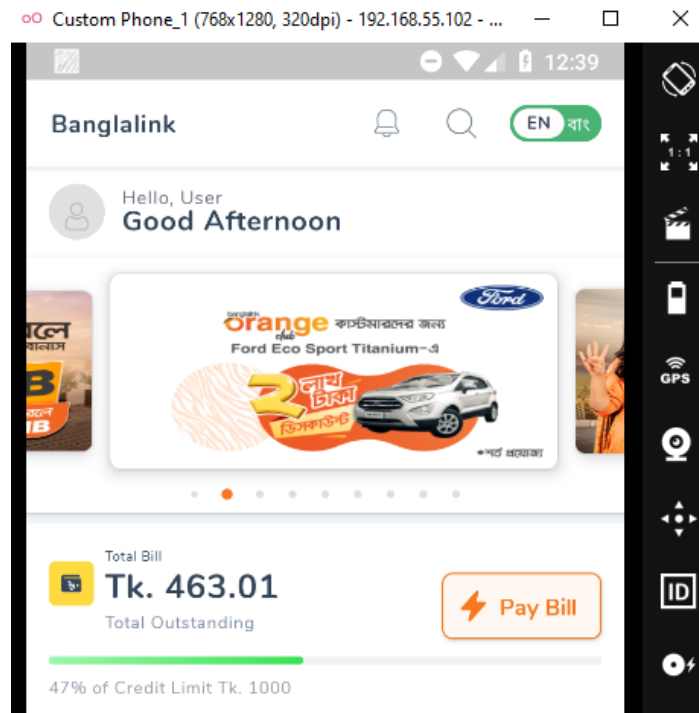


Figure 4.14: MyBL App On Genymotion

without any issue in Genymotion emulator rooted device and didn't show any alert.

Solution:

The app should detect and responds to the presence of a rooted or jailbroken device either by alerting the user or terminating the app.

4.14 The app does not prevent debugging and/or detects and responds when a debugger is attached.

Classification: Low Risk

CWE ID: 1244

Internal Asset Exposed to Unsafe Debug Access Level or State

OWASP MSTG-ID: MSTG-RESILIENCE-2

Description:

Permission mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad hoc access to specific pieces of data. It was observed that application has set insecure permissions, which will create security threat to an application.

Solution:

Some necessary protocols should be implemented for defence against common debugging tools.

[illegible]

Figure 4.15: Debugging Using ADB

5. Conculation

All the testings in this report were done based on the external knowledge of the web application as part of black-box testing. All the security issues discovered during that activity were explored and defined in this report. Please note that as technologies and risks alter over time, the vulnerabilities associated with the operation of systems described in this report and the actions necessary to reduce the exposure to such vulnerabilities will also change.