

# 777-Team

## 2022 Security Assessment Report Prepared For EAT ALLEY

The logo for EAT ALLEY, featuring the word "EAT" in black and "ALLEY" in black, with a blue stylized "A" in the middle.

Report Issued: 24/03/2022

<https://github.com/sudo-slingshot/AndroidERestaurantLECLECH>

---

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to **EatAlley** or facilitate attacks against **EatAlley**.*

***777-Team** shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on **EatAlley** 's environment. Any changes made to the environment during the period of testing may affect the results of the assessment. This pentesting report has been performed for educational purpose.*

# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b>	4
<b>HIGH LEVEL ASSESSMENT OVERVIEW</b>	5
Observed Security Strengths	5
Areas for Improvement	5
Short Term Recommendations	5
Long Term Recommendations	6
<b>SCOPE</b>	7
Networks and API	7
Other	7
Provided Credentials	
<b>OWASP RECOMMANDATIONS</b>	8
<b>TESTING METHODOLOGY</b>	9
<b>CLASSIFICATION DEFINITIONS</b>	10
Risk Classifications	10
Exploitation Likelihood Classifications	11
Business Impact Classifications	11
Remediation Difficulty Classifications	12
<b>ASSESSMENT FINDINGS</b>	13
<b>APPENDIX A - TOOLS USED</b>	15
<b>APPENDIX B - ENGAGEMENT INFORMATION</b>	16
Client Information	16
Version Information	16
Contact Information	16

## EXECUTIVE SUMMARY

**777-Team** performed a security assessment of the application **EatAlley** on 21/03/2022. **777-Team's** penetration test simulated an attack from an external threat actor attempting to gain access to systems within the **EatAlley's** android application. The purpose of this assessment was to discover and identify vulnerabilities in E-Restaurant Corp's infrastructure and suggest methods to remediate the vulnerabilities. **777-Team** identified a total of 4 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
1	0	2	1

The highest severity vulnerabilities give potential attackers the opportunity to access all confidential information of their users due to bad request management in API. To ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

**777-Team** identified the following strengths in E-Restaurant Corp's application. **EatAlley** should continue to monitor these controls to ensure they remain effective.

- No privacy tracker detected on app

## Areas for Improvement

**777-Team** recommends **EatAlley** takes the following actions to improve the security of the application. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack E-Restaurant Corp's information systems and/or reduce the impact of a successful attack.

## Short Term Recommendations

**777-Team** recommends **EatAlley** take the following actions as soon as possible to minimize business risk.

### Critical Warning: Requires immediate actions

- Encrypt / hash all the sensitive information / credentials on client side (primary to a major security update on the application)
  - The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, Download Manager, and Media Player. The default value for apps that target API level 27 or lower is "true". **Apps that target API level 28 or higher default to "false"** (which led us to think that the vendor modified this flag on purpose). The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and modify it without being detected
- Obfuscate the application source code.
- Deactivate debugs and backup from manifest to avoid apk pulling.

---

## Long Term Recommendations

**777-Team** recommends the following actions be taken over the next 6 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

### Security enhancement

- Secure the API to the latest transport security protocols. (Support HTTPS)
- Implement an efficient anti-root script to protect from data theft
- Rather than using shared preferences to store user's credential, prefer to use a database with access control.

## SCOPE

All testing was based on the scope as defined in the Request for Proposal (RFP) and official written communications. The items in scope are listed below.

### APIS and Network

APIS (IP)	Descriptions
217.160.0.150	test.api.catering.bluecodegames.com City: Karlsruhe (Germany)
216.58.207.228	Google.fr Country: United States of America Region: California City: Mountain View

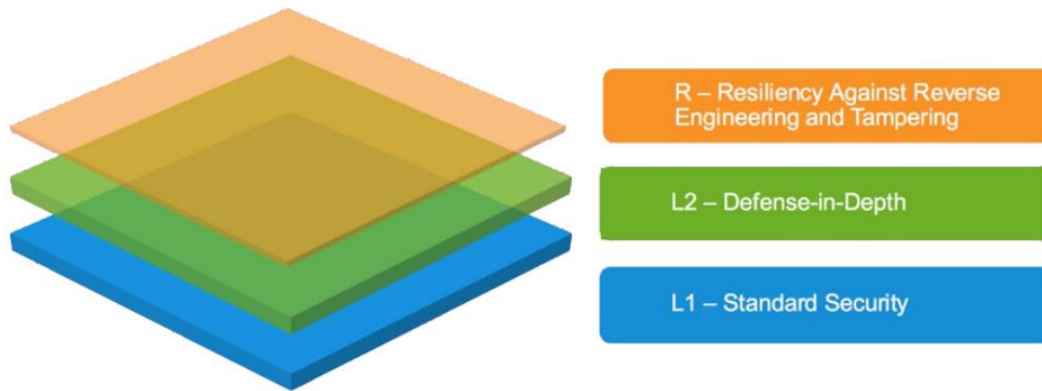
### Provided Credentials

**EatAlley** provided 777-Team with the following credentials and access to facilitate the security assessment listed below.

Item	Note
Customer Account	A fake customer account with password 'IamBatman' and email 'Bruce.Wayne@cityofgotham.us' for testing functionality that requires authentication.

# OWASP RECOMMENDATIONS

Based on OWASP we can make some recommendations to developers so they can continue to improve the application with a good security



*MASVS Layer (cc) OWASP*

Source : <https://www.softscheck.com/en/owasp-mobile-application-security-verification-standard-en/>

## Reminder

MASVS-L1 “Standard Security” defines a base of security requirements, e.g., that network traffic is completely protected by TLS and only a defined set of X.509 certificates of the endpoint is accepted. MASVS-L2 is based on these and defines additional requirements. For example, the specification of a two-factor authentication (2FA) or a renewed direct authentication before accessing sensitive data. Both levels can be additionally extended by MASVS-R “Resiliency Against Reverse Engineering and Tampering”. As the name suggests, the focus here is on protection against modifications and access to the app itself. Requirements from this level are, for example, that the app detects and reacts when it is started in an emulator or identifies and reacts to changes in code and data in its own memory area.



---

The selection of the correct level is determined by the respective protection requirements. For example, a games manufacturer may prefer apps MASVS-L1+R, since the standard security level is sufficient in this context, but resiliency is an important point to prevent or make changes to the app (e.g. cheating) more difficult.

The requirements for the levels MASVS-L1 and MASVS-L2 are divided into 7 categories from “Architecture, Design and Threat Modeling Requirements” to “Code Quality and Build Settings Requirements”. In each case, a base of requirements is defined according to MASVS-L1 and further requirements beyond that are specified according to MASVS-L2. In an eighth category, the resilience requirements are defined.

## Recommendations

The client's application should at least implement the L1, and R security levels based on the MASVS standard. Not being a banking application, it is not necessary in our opinion for the development team to implement advanced security (L2) such as staggered authentication.

## TESTING METHODOLOGY

**777-Team's** testing methodology was split into two phases: *Reconnaissance* and *Attack*. During reconnaissance, we gathered information about **EatAlley's** application systems. **777-Team** used different tools to scan the application's code and intercept the traffic. Next, we conducted our targeted assessment. **777-Team** gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

In our research phase we also analyzed the API. Despite the lack of public information, it seems that it is an educational API that does not care about security issues.

# CLASSIFICATION DEFINITIONS

## Risk Classifications

Level	Score	Description
<b>Critical</b>	<b>10</b>	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
<b>High</b>	<b>7-9</b>	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
<b>Medium</b>	<b>4-6</b>	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
<b>Low</b>	<b>1-3</b>	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
<b>Informational</b>	<b>0</b>	These findings have no clear threat to the organization but may cause business processes to function differently than desired or reveal sensitive information about the company.

## Exploitation Likelihood Classifications

Likelihood	Description
<b>Likely</b>	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
<b>Possible</b>	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
<b>Unlikely</b>	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

## Business Impact Classifications

Impact	Description
<b>Major</b>	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
<b>Moderate</b>	Successful exploitation may cause significant disruptions to non-critical business functions.
<b>Minor</b>	Successful exploitation may affect few users, without causing much disruption to routine business functions.

## Remediation Difficulty Classifications

Difficulty	Description
<b>Hard</b>	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
<b>Moderate</b>	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
<b>Easy</b>	Remediation can be accomplished in a short amount of time, with little difficulty.

## ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk
1	Clear text traffic	10	High
	User's credential storage	8	High
2	Backup and debug activated	7	Medium
3	Deprecated API version	6	Medium
4	Hardcoded information	5	Medium
5	Information log	2	Low

TEMPLATE NOTE: (Sorting by descending risk score)

# 1 - Vulnerability Finding

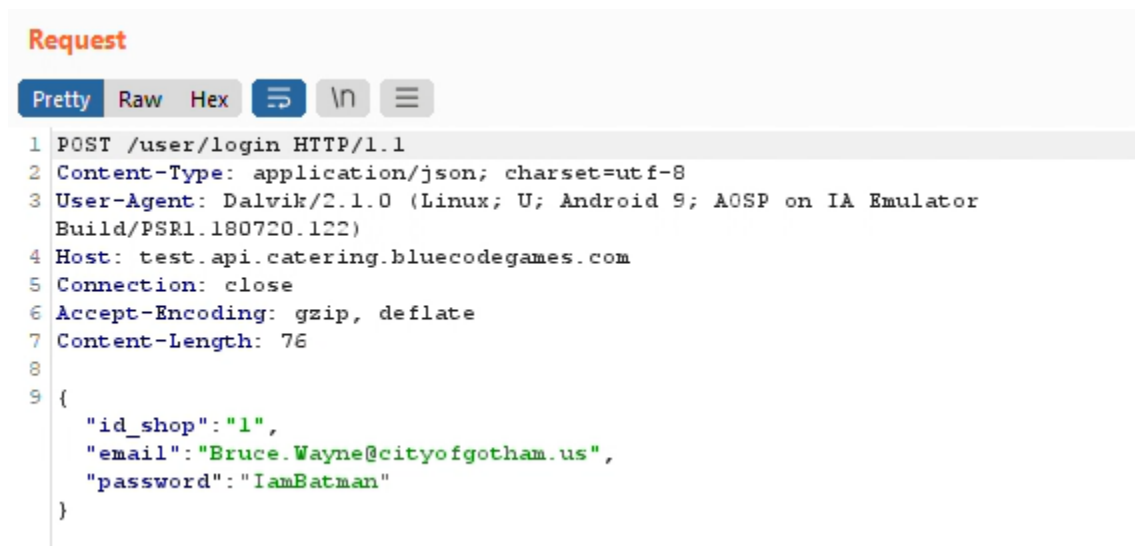
HIGH RISK (8/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Easy

## Security Implications

the security flaws that we have identified in the application can have a significant impact on our client's business model. By compressing user data and not securing command requests, the application exposes its users to theft or modification of data and a loss of trust.

## Analysis

Below you will find what we were able to do as attacker in the android application.



```
1 POST /user/login HTTP/1.1
2 Content-Type: application/json; charset=utf-8
3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; AOSP on IA Emulator
  Build/PSR1.180720.122)
4 Host: test.api.catering.bluecodegames.com
5 Connection: close
6 Accept-Encoding: gzip, deflate
7 Content-Length: 76
8
9 {
  "id_shop": "1",
  "email": "Bruce.Wayne@cityofgotham.us",
  "password": "IamBatman"
}
```

**Figure 2.3.1:** Using credential in clear text

A terminal window with a dark background and light-colored text. The text shows the output of the 'drozer' tool. It starts with 'drozer Console (v2.4.4)', followed by two commands: 'dz> run app.package.list -f erestaurant' and 'dz> run app.package.attacksurface fr.isen.leclech.androiderestaurant'. The output for the second command is 'Attack Surface:' followed by a list of exported components: '1 activities exported', '0 broadcast receivers exported', '0 content providers exported', '0 services exported', and 'is debuggable'.

```
drozer Console (v2.4.4)
dz> run app.package.list -f erestaurant
fr.isen.leclech.androiderestaurant (EatAlley)
dz> run app.package.attacksurface fr.isen.leclech.androiderestaurant
Attack Surface:
  1 activities exported
  0 broadcast receivers exported
  0 content providers exported
  0 services exported
  is debuggable
```

*Figure 2.3.2: Using drozer in surface attack mode*

#### References (opt)

- <https://github.com/Sevaarcen/RADAR/tree/master/radar/playbooks>
- <https://owasp.org/www-project-top-ten/>

## APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
<b>BurpSuite Community Edition</b>	Used for testing of API requests
<b>Drozer</b>	Used to find exploits (with scripts)
<b>Jadx</b>	Used to analyze the code and find data in app
<b>Android Emulator</b>	Used to run the app and test it as a customer

**Table A.1:** Tools used during assessment

## APPENDIX B - ENGAGEMENT INFORMATION

### Client Information

<b>Client</b>	E-Restaurant Corp
<b>Approvers</b>	The following people are authorized to change the scope of engagement and modify the terms of the engagement <ul style="list-style-type: none"><li>Yohan LE CLECH, Jean-Christophe TURCAT, Paul-Emile NEU</li></ul>

### Version Information

Version	Date	Description
1.0	22/03/2022	Initial report to client

### Contact Information

<b>Name</b>	777-TeamConsulting
<b>Address</b>	Maison du numérique et de l'innovation, Pl. Georges Pompidou, 83000 Toulon