Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 179 (2021) 962–965

Procedia Computer Science

www.elsevier.com/locate/procedia

5th International Conference on Computer Science and Computational Intelligence 2020

Peeking and Testing Broken Object Level Authorization Vulnerability onto E-Commerce and E-Banking Mobile Applications

Anthony Viriya[a], Yohan Muliono[b,*]

[a]*Consultant Penetration Tester, Penetration Testing Department, The ITSEC Group, Jakarta, Indonesia 12950*
[b]*Cyber Security Program, Computer Science Department, Bina Nusantara University, Jakarta, Indonesia 11480*

Abstract

Internet traffic is already a daily usage and unavoidable for many people, moreover, people needs it anywhere and anytime, so that more companies tend to fulfill that desire onto bringing some of the application to mobile devices. This research aim to find out whether the mobile application security has been the prioritize for the company or not. Several mobile applications has been tested ethically and legal in two impactful industries in Indonesia, E-Commerce and Banking. Several findings has been found in the mobile application just tested by using Broken Object Level Authorization which is the first point of top ten OWASP vulnerabilities. All attacks conducted are not complicated to reproduce, malicious user only need to know the basic of request interception in mobile phone or web application, the attack could be done by using any free proxy software. High dependency only on Jailbreak Detection, Root Detection and SSL Pinning as the main security protocol is not a wise decision to be taken.

Keywords: Type your keywords here, separated by semicolons ; cyber security; mobile security; penetration testing

1. Introduction

Mobile internet traffic is a huge and unavoidable thing, almost all transactions made could be carried out through the mobile network (social network services, e-commerce, banking etc.) almost every aspects in our daily life could be easily done by just using mobile phone [1]. Prediction has been made since 2017 through 2022 mobile internet traffic will be exponentially increasing by seven fold and will dominate the internet traffic in the world [2]. Therefore, application developers will be urge to port every possible application to mobile application. Some industries had already did improve their mobile application to compete in this digital era, especially industry such as banking, e-commerce, games, etc [3]. Consumers nowadays desire a privilege to access application wherever and whenever they want to, they

* Corresponding author. Tel.: +62-813-1555-6813
E-mail address: ymuliono@binus.edu

1877-0509
10.1016/j.procs.2021.01.101

can shop virtually anywhere and anytime, playing online games when they have to wait for something or wire some money in 2 A.M. is naturally ordinary activity for some people.

Despite of the functionality of the mobile application developed these days, did security become one of the main issues? Recently a research conducted to determine whether security is matter for some companies, the result shows that security still not a big deal for some companies. They tend to deliver applications in a short time with full concern only on the functionalities, with not paying much attention for the security itself[4].

based on research conducted by kellner et al.[5], they state that an iOS application with no jailbreak detection could be tampered and utilized in malicious way to harm other users. Several findings that will be explained in later sections found that mobile applications tend to depends on jailbreak detection, root detection and SSL pinning. Once the jailbreak detection, root detection and SSL pinning could be bypassed, the application never being tested nor patched according to proper security testing guide such as OWASP. In fact, more than hundreds of methods can be used to perform attacks in mobile application, this research aims to prove whether using one of the most well-known methods (Broken Object Level Authorization) and find out whether the company is aware of this method and protected its mobile applications against this method.

1.1. Jailbreak Detection, Root Detection and SSL Pinnning

Jailbreak detection is a mechanism that could detect whether the user of the application in iOS phone is in root privilege or not and root detection is the same detect mechanism and work in Android phone. SSL pinning is a security mechanism that could be used in client side to avoid interception using third party application by validating the server certificates after SSL handshake protocol. These mechanism are often used by developers as their only security mechanism, due to the great reliance on these methods. The developers never performs penetration testing of the application directly, Therefore, when these defense mechanism(Jailbreak Detection, Root Detection, SSL Pinnning) failed, the application behind these mechanisms is not ready to receive attacks since no penetration testing has been performed before.

2. OWASP

The Open Web Application Security Project (OWASP) is an open community which dedicated to improve security measurement in many aspects like web and mobile application[6], OWASP is a community based guideline globally used by many penetration tester[7][8][9] to test whether their application is already appropriate according to the standard measurement of OWASP. OWASP foundation released many publications in security testing guidelines for example: Web Security Testing Guide, Mobile Security Testing Guide and API Security Testing Guide where could be downloaded free and could become a standard security testing in applications. For each of them, OWASP has rank all the vulnerabilities into top ten every year and every two year for website.

3. Broken Object Level Authorization

According to OWASP API Security Top ten 2019[10], the number one in rank is Broken Object Level Authorization where system could not give a proper authorization for the data requested by inappropriate user. API endpoint supposed to check every function which contains object level authorization that accesses a data source using an input from the user. This research will perform this attack to test against several mobile applications in Indonesia, because this attack has been assessed as the most proven attack in 2019.

3.1. Attack Scenario

A server that hosting an e-commerce service for everyday goods provides a buy and sell features for sellers and consumers. when consumers want to buy an item, the customers should choose the product, enter the product into the cart then finish the payment. after that, the seller will receive an purchase order but not the money yet, prepare the goods from the purchase order and proceed to the delivery done by third party. then after the delivery completed, the customer should check every item they received if the customer have any complaint, they have rights to not complete

the transactions and raise the issue, so the money will not wired yet to the sellers, but if the customer do not have any issue, the customer should click the transaction complete button, the transaction between the seller and customer finished and the money will be wired to the seller. The attack scenario here is, how if the seller sent a piece of stone to every order received by the seller, and the seller pretend to be customer and hit the API that supposed to be accessed only by specific customer, because of the Broken Authorization, money will be wired even though the customer do not press the transaction complete.

4. Attack Method and Results

According to the attack scenario, an attack would be conducted against several mobile application, the test would be conducted ethically against each of the company's applications tested. Attack will be conducted in three sectors of applications which involving money in the daily transaction including e-commerce and e-banking. Broken Object Level Authorization will be conducted in the applications in every function possible.

4.1. Broken Object Level Authorization against E-Commerce Application

This Attack conducted in an ethical manner where this company have a policy for bug bounty, means a bug that could be found in the application and reported without being exploited will be rewarded by the company. Vulnerability found in one of the biggest E-commerce company in Indonesia, the vulnerability found make malicious user can bypass authorization occured in a transaction, where the sellers could finish the transaction without the customers consent, the transaction completion policy in the E-commerce is whether the user click the transaction complete button, or after five days after the items being delivered to the user but the user do not click the transaction complete button nor complaint about the items, the system will complete the transaction automatically. The API request without proper authorization found at https://{E-CommerceName}/reputationapp/review/api/v2/edit/validate through that link, the user could edit the user ID and finish the transaction without user consent. Report for this attack has been reported and remediated by the company.

4.2. Broken Object Level Authorization leads to Account Takeover in E-Commerce Application

This Attack conducted in a same ethical manner with the first attack where the company have a legal bug bounty program. The Tokopedia iOS application's OTP can be bypassed using several vulnerability chaining such from weak SSL Pinning that can by bypassed using a free cydia tweak (could be downloaded freely) and No Jailbreak Detection. Vulnerability could be produced by copying a legitimate response after submitting correct OTP. After that we can send any request that needs OTP for verification, such as forgot password and send the OTP through the mobile phone, next we will intercept the request, and changing the response using a valid response we copy beforehand, finally the request completed successfully even though we did not input a correct OTP. Report for this attack has been reported and remediated by the company.

4.3. Broken Object Level Authorization against E-Banking Application

This testing occured whereas one of the researcher works in a cyber security consultant company, this application is one of the penetration testing project which conducted in ethical manner with a legal consent between the client and penetration tester, thus the name and URL would be blurred. One of the E-Banking could be exploited through arbitrary source account to buy a cellphone credit through API URL: https://{bank-name}/v2/purchase/{API-name} when this URL is accessed through third party interceptor such as burp, the application would requesting several parameters:

- origin_account_number = sender account number
- provider = telephone provider
- destination_phone = user mobile phone number which should be receiving the phone credit
- transaction_token = token generated by API

by editing the origin_account_number parameter, malicious user could use any valid account number and buy the cellphone credit using another user account number without the user consent. Report for this attack has been reported and being remediated by the company.

5. Attack Summary

Three attacks that has been conducted are not that complicated to reproduce, the attacker just have to know the basic of intercepting request in mobile phone or web application, the attack could be done by using free proxy software such as Burp Suite and Fiddler. The idea of having a Jailbreak Detection, Root Detection and SSL Pinning for the only security solution is not a wise idea to implement. Jailbreak detection of banking apps could easily be evaded, almost every banking application jailbreak detection mechanism could be evaded even though the application located in the top applications used[5]. But, to use Jailbreak Detection, Root Detection and SSL Pinning as an additional layer of mobile security is a must thing to do.

6. Conclusion and Future Work

The Conclusion is, Well-known mobile application can be abused even using only one method, whereas in fact, there are more than hundreds of methods can be performed. Furthermore, what happens if the company relies only on Jailbreak Detection, Root Detection and SSL Pinnning mechanism? if the mechanism failed, afterwards, the application can easily be abused. Even though the application is made by a well-known company, it does not rule out that security holes still exist in the application. All the attacks conducted in many E-commerce and banking, not all of them vulnerable against Broken Object Level Authorization. In surprise, some of the applications could be easily exploited without much effort. Moreover, one of the application already has the feature for more than two years after tracing back the details of update in AppStore, it means, the bug already sitting there for two years. For the future work, this research will lead to combine this work with the research conducted by Kellner et al[5]. Future research will be conducted by trying to evade the jailbreak or root detection and SSL Pinning for top e-banking, e-commerce and another applications which are famous in Indonesia and has money transaction inside the applications. Next, the research will conduct other Top Ten Security indexed by OWASP from Mobile or API to reach a conclusion whether mobile applications in Indonesia too dependent in root detetion, jailbreak detection and SSL Pinning without paying attention to apply secure code in the application or jailbreak detection, root detection and SSL pinning are additional layer of security.

References

1. Yesilyurt, M., Yalman, Y.. Security threats on mobile devices and their effects: estimations for the future. *International Journal of Security and Its Applications* 2016;**10**(2):13–26.
2. Forecast, G.M.D.T.. Cisco visual networking index: global mobile data traffic forecast update, 2017–2022. *Update* 2019;**2017**:2022.
3. Reaves, B., Bowers, J., Scaife, N., Bates, A., Bhartiya, A., Traynor, P., et al. Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications. *ACM Transactions on Privacy and Security (TOPS)* 2017;**20**(3):1–31.
4. Sϕhoel, H., Jaatun, M.G., Boyd, C.. Owasp top 10-do startups care? In: *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE; 2018, p. 1–8.
5. Kellner, A., Horlboge, M., Rieck, K., Wressnegger, C.. False sense of security: A study on the effectivity of jailbreak detection in banking apps. In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE; 2019, p. 1–14.
6. OWASP, . *OWASP Foundation*; 2020 (accessed August 12, 2020). URL https://owasp.org/.
7. Holik, F., Horalek, J., Marik, O., Neradova, S., Zitta, S.. Effective penetration testing with metasploit framework and methodologies. In: *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*. IEEE; 2014, p. 237–242.
8. Pratama, I.P.A.E., Wiradarma, A.A.B.A.. Open source intelligence testing using the owasp version 4 framework at the information gathering stage (case study: X company). *International Journal of Computer Network and Information Security* 2019;**11**(7):8.
9. Li, J.. Vulnerabilities mapping based on owasp-sans: A survey for static application security testing (sast) 2020;.
10. OWASP, . *OWASP API Security Top 10 2019*; 2019 (accessed August 12, 2020). URL https://owasp.org/www-project-api-security/.